

Florida Health Care Connections (FX)
MMIS Concept of Operations
(MMIS ConOps)

Version: 200
Last Modified: April 28, 2020

Document Number: [Phase III: IS/IP, EDW, and Provider v200](#)

REVISION HISTORY

Version	Date	Description of Changes
001	01/09/2019	Draft Submission to Agency
002	02/12/2019	Submission to Agency for Final Approval
100	02/26/2019	Approved Final Version
101	04/03/2020	Draft Submission to Agency
200	04/28/2020	Approved Final Version 200

TABLE OF CONTENTS

SECTION 1	INTRODUCTION.....	1
SECTION 2	REFERENCED DOCUMENTS	4
2.1	CURRENT SYSTEM.....	4
2.1.1	<i>Functional Description</i>	<i>4</i>
2.1.2	<i>User Community Description.....</i>	<i>5</i>
2.1.3	<i>Technical Architecture</i>	<i>6</i>
SECTION 3	GOALS, OBJECTIVES, AND RATIONALE FOR NEW OR SIGNIFICANTLY MODIFIED SYSTEM.....	9
3.1	PROJECT PURPOSE	9
3.1.1	<i>System Goals and Objectives</i>	<i>16</i>
3.2	PROPOSED SYSTEM.....	19
3.2.1	<i>System Scope</i>	<i>21</i>
3.2.2	<i>Business Processes Supported</i>	<i>21</i>
3.2.3	<i>High Level Functional Requirements.....</i>	<i>22</i>
SECTION 4	SCENARIOS ANALYSIS.....	26
SECTION 5	FACTORS INFLUENCING TECHNICAL DESIGN	33
5.1	RELEVANT STANDARDS.....	33
5.2	ASSUMPTIONS, DEPENDENCIES, AND CONSTRAINTS.....	33
5.3	AGENCY GOALS AND OBJECTIVES	36
5.4	DESIGN GOALS	37
SECTION 6	PROPOSED SYSTEM	39
6.1	TECHNICAL SOLUTION ALTERNATIVES	39
6.2	RATIONALE FOR SELECTION	41
6.3	RECOMMENDED TECHNICAL SOLUTION.....	42
6.4	PROPOSED SOLUTION DESCRIPTION.....	45
6.5	CONTEXT DIAGRAM.....	45
6.6	HIGH-LEVEL OPERATIONAL REQUIREMENTS AND CHARACTERISTICS	46
6.6.1	<i>User Community Description.....</i>	<i>46</i>
6.6.2	<i>Non-Functional Requirements</i>	<i>47</i>
6.7	HIGH LEVEL ARCHITECTURE & ALTERNATIVES ANALYSIS.....	52
6.7.1	<i>Application Architecture</i>	<i>57</i>
6.7.2	<i>Information Architecture.....</i>	<i>58</i>
6.7.3	<i>Interface Architecture</i>	<i>62</i>
6.7.4	<i>Technology Architecture</i>	<i>63</i>
6.7.5	<i>Security and Privacy Architecture</i>	<i>65</i>
SECTION 7	ANALYSIS OF THE PROPOSED SYSTEM	68
7.1	IMPACT ANALYSIS	68
7.1.1	<i>Operational Impacts.....</i>	<i>68</i>

7.1.2 *Organizational Impacts*..... 69

7.1.3 *Risks* 70

7.1.4 *Monitoring and Controlling Risk*..... 73

7.1.5 *Issues to Resolve* 75

7.1.6 *Critical Success Factors for Remainder of Project*..... 76

SECTION 8 GLOSSARY.....78

SECTION 9 APPENDICES81

LIST OF FIGURES

Figure 1: Strategic Refresh Methodology	3
Figure 2: Medicaid Ecosystem.....	5
Figure 3: Current Conceptual Technical Architecture	8
Figure 4: Phase III: FX FMMIS Resolution	12
Figure 5: Phase IV: Remaining Non-FMMIS Modules.....	15
Figure 6: FX Strategy Articulation Map.....	19
Figure 7: FX Modular Transformation	20
Figure 8: FX Transformation Model.....	25
Figure 9: FX Transformation Foundation.....	26
Figure 10: Project Portfolio Management.....	30
Figure 11: TSRG Standards Hierarchy Example.....	33
Figure 12: Other State Transformation Themes	40
Figure 13: Context Diagram	45
Figure 14: Conceptual Technical Architecture Diagram	57
Figure 15: Multilayer Application Architecture Model.....	58
Figure 16: National Information Exchange Model.....	60
Figure 17: Conceptual Data Model Sample.....	61
Figure 18: Conceptual View of Multiple Environments.....	64
Figure 19: FX Security Description.....	67

LIST OF TABLES

Table 1: Supported Business Processes	22
Table 2: FX Implementation Approach Alternatives.....	41
Table 3: User Community Description	47
Table 4: Security and Privacy Standards	49
Table 5: System Availability Requirements	50
Table 6: Current Volumetric Capacity.....	50
Table 7: Performance Expectations	51
Table 8: Solution Design Alternatives	56
Table 9: MMIS Interfaces	63
Table 10: Probability of Occurrence.....	71
Table 11: Impact on Projects	72
Table 12: Calculated Risk Exposure.....	72
Table 13: Risk Management Activities.....	75
Table 14: Critical Success Factors	77

SECTION 1 INTRODUCTION

The Florida Agency for Health Care Administration (AHCA or Agency) is continually looking to fulfill its mission *to Drive transformation of the health care system to increase accountability through improved health outcomes with efficient and effective use of taxpayer resources*. As part of this mission, the Agency is transforming the Medicaid Enterprise System (MES), the group of systems that deliver Medicaid Program services.

This project was initiated as the MES Re-Procurement Project in May 2015 to replace the Florida Medicaid Management Information System (FMMIS). Under the FMMIS re-procurement project, the Agency proposed a takeover procurement of the FMMIS, replacement of the Decision Support System (DSS), and combined Fiscal Agent (FA) and Systems Integrator (SI) services. The Agency submitted the FMMIS/DSS/FA/SI Invitation to Negotiate (ITN) document to the Centers for Medicare and Medicaid Services (CMS) on October 7, 2015, for review and approval.

On November 30, 2015, CMS issued a Request for Additional Information (RAI) letter requiring the Agency to solicit a separate vendor for SI services as a requirement for Florida to obtain enhanced Federal Financial Participation (FFP). This new direction from CMS was a departure from the approved Planning Advance Planning Document (PAPD), Implementation Advance Planning Document (IAPD), and previously held discussions with CMS. On February 9, 2016, CMS issued a formal disapproval letter to the Agency for the FMMIS/DSS/FA/SI ITN.

In December 2015, CMS released the Medicaid Program Final Rule: Mechanized Claims Processing and Information Retrieval Systems (CMS 2392-F). This final rule modified regulations pertaining to 42 Code of Federal Regulations (CFR) 433 and 45 CFR 95.611, effective January 1, 2016. Among other changes, this final rule requires states to follow a modular approach to Medicaid Information Technology (IT) acquisition to increase the opportunity to select progressive technology from different vendors and avoid vendor lock-in and the risks associated with a single, monolithic solution. The modular approach supports the use of open source and proprietary commercial off-the-shelf (COTS) software solutions over the use of custom solutions, thereby reducing the need for custom development. The conditions of modularity and interoperability must be met for states to qualify for enhanced FFP.

Considering the emerging guidance from CMS, the Agency released an initial Florida MES Procurement Strategy reflecting a modular approach on May 2, 2016. On November 22, 2016, the Agency submitted an updated Implementation Advance Planning Document (IAPDU) request for enhanced FFP for the Florida FX (formerly MES) Procurement Strategy. The Agency's IAPDU was approved by CMS on December 21, 2016.

In July 2018, the Agency rebranded the Florida MES transformation to Florida Health Care Connections (FX).

The Agency completed a purposeful and deliberate exercise to refresh its 2017 strategy following Phase II to focus on the resolution of the Fiscal Agent contract and continuing operations.

The original FX Strategic Plan was driven by a group of guiding principles agreed upon by Executive staff that aligned to the Agency's mission under the prior administration. The goal of the 2019 strategic refresh was to ensure that the FX Project and the roadmap for implementation was still aligned to the mission and strategic priorities of the Governor, Legislature, and Executive Leadership of the Agency and to make the needed modifications to adapt to any variance.

In addition, the Medicaid Management Information System (MMIS) market has been changing and innovating since CMS issued its modularity guidance to states. AHCA's desire is to take advantage of these ongoing innovations even while implementing the early components and modules of FX. The Agency has also learned a great deal in the first two years of this transformation and experienced some internal change as well. For example, early conversations with other Health and Human Services (HHS) agencies revealed that interoperability is more complex than initially anticipated but still represents enormous potential for efficiencies for the State. The Agency also welcomed its new Secretary in 2019 and updated its mission and vision in the most recent Long-Range Program Plan.

To take advantage of new innovations as they become commercially available and to incorporate this new knowledge and Agency transition, the 2019 strategy refresh focused on incorporating all of this context into the planning, procurement strategy, and scope of the FX modules while maintaining the long-term FX Vision. This work began in October 2019 and culminated with an approved plan for the FX procurement strategy in early 2020 using a five-step process.

The first step of the refresh process was an assessment of the current state to identify and validate previous findings on the pain points, process gaps, and project opportunities facing the Agency and provided a foundational understanding of the current operations at the Agency. This translated into steps two and three that were primarily focused on the validation of and alignment to the FX Vision / Guiding Principles and identifying any changes since 2017 to the strategic priorities for the Agency through executive sessions. These sessions served as the primary building blocks to guide the decision-making in step four where the projects identified in step one were prioritized. The prioritized modules and sequencing decisions were then used to generate the draft FX procurement strategy roadmap options. The fifth and final step focused on validation of the recommended roadmap option with the Agency to gain alignment and buy-in from executives and the Secretary. **Figure 1: Strategic Refresh Methodology** depicts the refresh process.

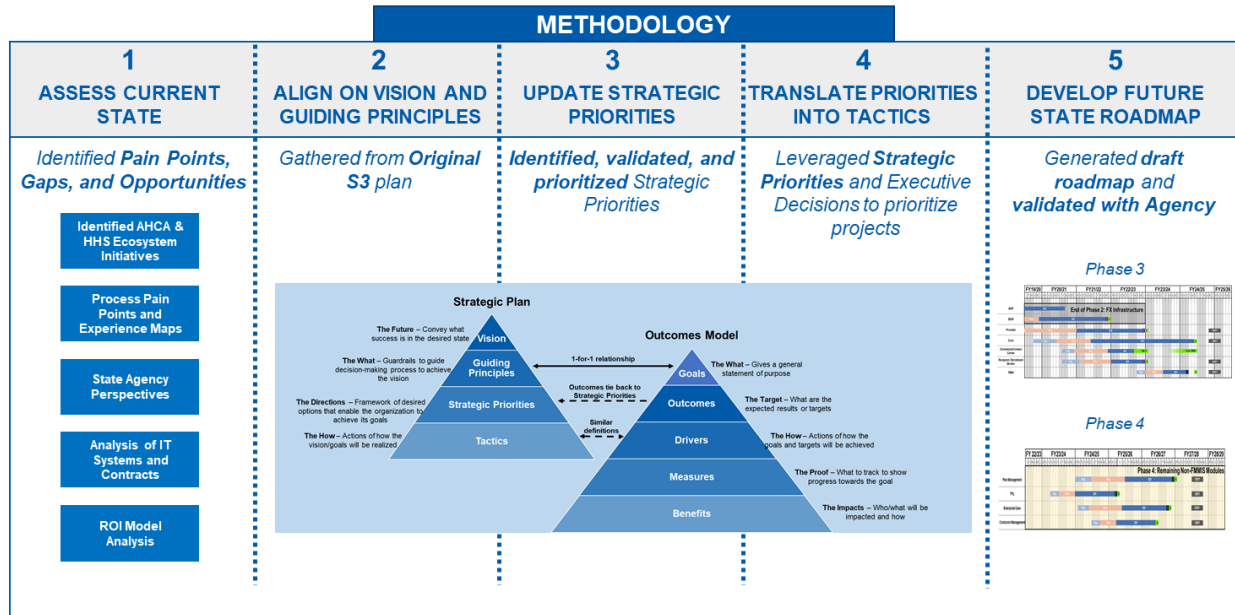


Figure 1: Strategic Refresh Methodology

This strategy refresh process led to a streamlined set of projects to be completed by December 2024 while allowing additional transformational initiatives to follow in a final FX Phase IV. All four phases of the refreshed FX procurement strategy are covered in detail in Section 3.1 of this document.

The FX procurement strategy aligns to CMS Standards and Conditions to ultimately transition to an interoperable and unified Medicaid Enterprise where individual processes, modules, sub-systems, and systems work together to support the Medicaid program. This approach is intended to provide the most efficient and cost-effective long-term solution for FX while complying with federal regulations, achieving federal certification, and obtaining enhanced federal funding.

SECTION 2 REFERENCED DOCUMENTS

The following documents were referenced in the development of the Florida MMIS Concept of Operations.

- Florida MES Procurement Strategy
- Approved Planning Advanced Planning Document Update (PAPDU)
- EDW Project Partnership Understanding
- MITA Concept of Operations and Addendum
- P-1: Revised MITA State Self-Assessment and Update Process
- P-2: FX Project Management Standards
- S-3: Enterprise Systems Strategic Plan and Refresh
- S-4: Strategic Project Portfolio Management Plan
- T-1: Data Management Strategy
- T-2: Information Architecture Documentation
- T-4: Technical Management Strategy
- T-5: Technical Architecture Documentation
- T-6: Technology Standards
- T-7: Design and Implementation Management Standards
- T-8: Enterprise Data Security Plan
- Integration Services and Integration Platform Invitation to Negotiate
- Enterprise Data Warehouse Invitation to Negotiate
- Provider Management Module Business Case
- Schedule IV-B Fiscal Year (FY) 2020-21

2.1 CURRENT SYSTEM

2.1.1 FUNCTIONAL DESCRIPTION

The Florida Medicaid Enterprise System is a collection of many systems, each with its own platform, systems architecture, and proprietary data stores. The systems in the MES are islands of processing and information. Data exchange provides the bridge between these systems. The current Medicaid Enterprise uses the MMIS and multiple systems and functions integrated or interfacing with the MMIS, such as the Automated Health Solutions (AHS) HealthTrack system, the Health Information Exchange (HIE), the Federally Facilitated Marketplace (FFM), and care management organization systems.

Figure 2: Medicaid **Ecosystem** summarizes Florida's MMIS which encompasses mission critical business systems upon which the Medicaid Enterprise and Medicaid ecosystem depend.

This current state can be categorized as follows:

- Providers, health plans, and Agency systems primarily submit information to MMIS through Electronic Data Interchange (EDI) and Secure File Transfer Protocol (SFTP) batch transmissions
- Pharmacy Benefits is operated by an outside vendor, Magellan

- The enrollment broker vendor is AHS. AHS operates both the Choice Counseling call center to enroll recipients in health plans and the Provider Network Verification (PNV) system to monitor health plan provider networks’ adequacy
- Other Florida agencies perform Medicaid processes using replicated Medicaid data; primarily using batch interfaces
- The Decision Support System (DSS) is the data warehouse that supports analytics, ad hoc inquiry and management, and administrative reporting
- The HIE system enables provider-to-provider exchange of information
- The system lacks a 360-degree view of recipient information or alerting of changes in social determinants of health data

MEDICAID ECOSYSTEM – Stakeholders and Other entities

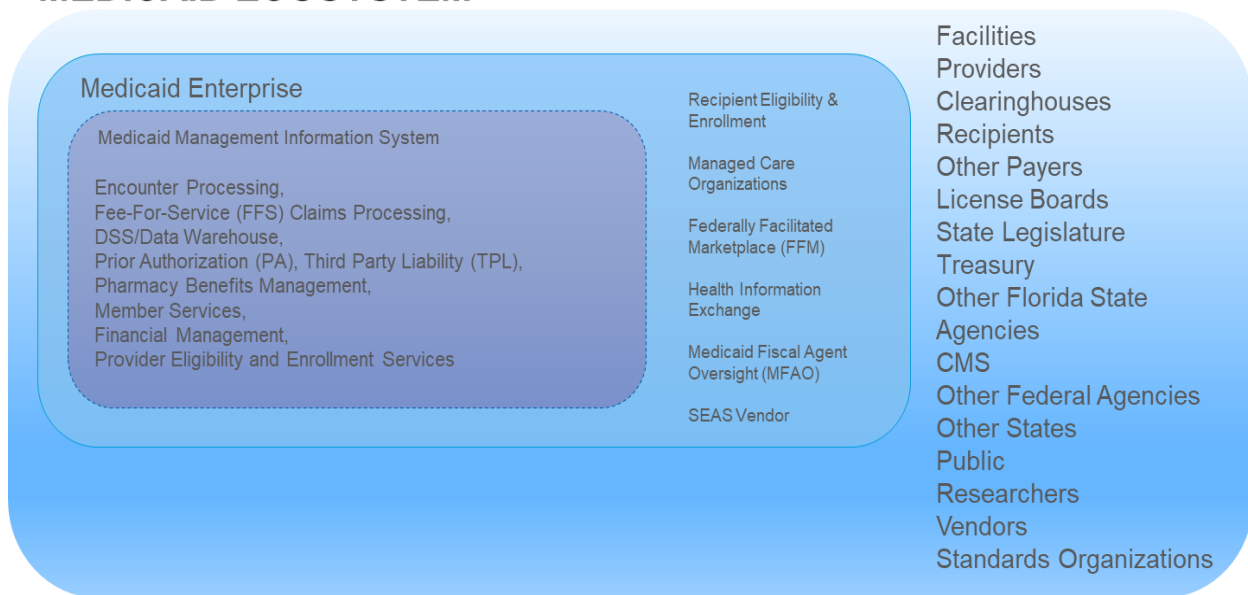


Figure 2: Medicaid Ecosystem

2.1.2 USER COMMUNITY DESCRIPTION

Listed below is the description of the user community:

- Agency staff access the MMIS to perform assigned daily activities. These include, but are not limited to, assisting members with questions about benefits and enrollment, billing issue resolution for Medicaid providers, enrollment for new providers into the Medicaid program, and creation of new accounts receivables and expenditures
- Other Agency staff access the MMIS and DSS to complete tasks such as researching Medicaid eligibility, assisting with system change requests, and gathering data for use in fraud and abuse determinations
- External organizations access the MMIS to update eligibility spans, submit claims, verify Medicaid eligibility, and identify potential fraud

- Providers access the MMIS for multiple reasons such as enrolling as a Medicaid provider, verification of recipient eligibility, claims submission, and confirmation of claim payment status
- Billing Agents submit claims on behalf of Medicaid providers through various clearinghouses for processing by MMIS
- Health plans access the MMIS to verify Medicaid eligibility, submit encounter transactions, and to research encounter errors
- Agency staff use DSS and its components for data needs that include but are not limited to analyzing data for the impact of policy changes, forecasting, program performance, and reporting information to all stakeholders including CMS
- Other Agency staff access DSS to verify data integrity, research data issues, forecast program expenditures, and provide ad hoc data requests for other internal and external entities
- External organizations and community partners access DSS to obtain reports and datasets for a variety of research and/or litigations involving Medicaid membership

2.1.3 TECHNICAL ARCHITECTURE

The information technology that supports the operation of the Medicaid program is distributed across many state agencies, health plans, and provider systems. There are hundreds of state agency computer systems and thousands of provider systems that must work together to deliver healthcare services to the people of Florida. In this highly distributed technology landscape, there is substantial duplication and inconsistencies of information and processing across systems.

Currently ten state agencies have direct responsibilities in processing or supporting the operation of the Medicaid program. Within the Agency alone, there are more than 140 computer systems or applications in operation. More than 80 of these systems play a direct role supporting the operation of the Medicaid program. A complete list of MMIS interfaces can be found in Appendix D.

The current Medicaid Enterprise contains several primary components including EDI, the MMIS/DSS, interChange User Interface (UI), and the Prescription Benefits Management System (PBMS), all of which are built around Service Oriented Architecture (SOA) principles.

EDI manages the flow of the various X12 transactions into and out of the Medicaid Enterprise. EDI utilizes BizTalk and Simple Object Access Protocol (SOAP) servers, mapping X12 transactions into proprietary XML file structures for processing in the MMIS.

The largest system in the Medicaid Enterprise is the MMIS/DSS, currently operated by the Fiscal Agent, DXC Enterprise Systems, LLC. The MMIS components of the system are comprised primarily of a collection of custom-built software applications used for processing Medicaid claims and encounter transactions. This processing includes the adjudication of claims and encounter transactions via batch processes and online submissions, the processing of financial transactions, producing and distributing payments, the storing and utilization of provider and recipient enrollment and demographic data, and the implementation of business rules and supporting reference data.

The DSS components of the system are comprised of a collection of Extract, Transform, and Load (ETL) programs written in the C programming language, a set of Business Intelligence tools, and an Oracle database. The DSS provides the tools necessary for analytics and reporting.

The technologies utilized in the implementation of the MMIS/DSS include Windows and HP-UX operating systems; Oracle and SQL Server databases; Commercial-off-the-Shelf (COTS) products such as Business Objects, Crystal Reports, SPSS, and ArcView GIS; and programming languages include C, C#, VB.NET, Javascript, Perl, VBScript, R and SAS. The MMIS/DSS system is hosted at a commercial data center in Orlando, Florida.

The interChange User Interface (UI) is a web-based solution developed with Microsoft.NET technologies. The UI allows highly detailed access to all Claims, Provider, Recipient, Financial, and Reference data stored in the MMIS. Authorized users also have update capabilities to relevant data.

The Prescription Benefits Management System (PBMS) is a Point-of-Sale (POS) Pharmacy Claims processing system operated and maintained by Magellan Health Services. Currently the PBMS is comprised of proprietary software running on a UNIX platform with an Oracle database from a data center in Maryland Heights, Missouri. This system receives and adjudicates POS NCPDP D.0 claims transactions which are subsequently transmitted via SFTP to the MMIS for payment. Users interact with pharmacy data via interChange or by means of FirstRx, a proprietary user interface operated by Magellan Health Services.

The number of agencies and systems that access and manage data used for healthcare delivery is likely to expand significantly. These agencies exert significant effort processing system-to-system interfaces to extract, load, and update information in one system with information from another system. Because of the many systems in operation, there is not a reliable *single source of truth* to make processing, reporting, policy analysis, investigation, or analytic decisions. Differences in data timeliness, data validation, data transformation, and application of policy within systems means reports and data analysis vary depending on which system performs the analysis.

Figure 3: Current Conceptual Technical Architecture provides a current state overview of the major components of the MMIS/DSS systems and interfaces with those systems.

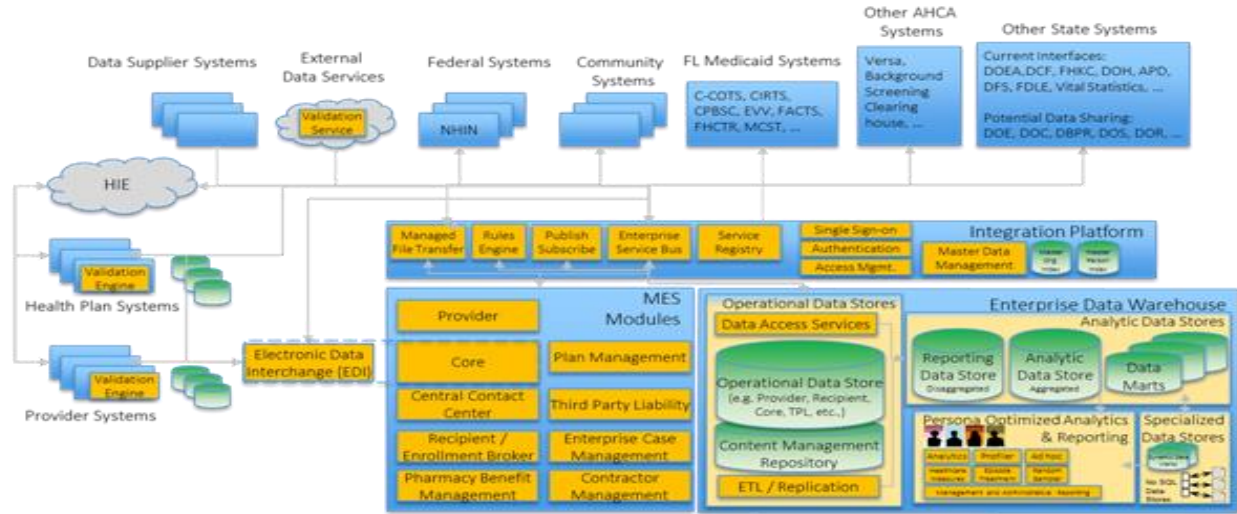


Figure 3: Current Conceptual Technical Architecture

SECTION 3 GOALS, OBJECTIVES, AND RATIONALE FOR NEW OR SIGNIFICANTLY MODIFIED SYSTEM

3.1 PROJECT PURPOSE

The FX procurement strategy proposed a phased approach to replace the current functions of the FMMIS based on the CMS Standards and Conditions to ultimately transition to an interoperable and unified Medicaid Enterprise where individual processes, modules, sub-systems, and systems work together to support the Medicaid program. This approach is intended to provide the most efficient and cost-effective long-term solution for FX while complying with federal regulations, achieving federal certification, and obtaining enhanced federal funding. The four phases of the FX procurement strategy are covered in detail below:

PHASE I: PROFESSIONAL SERVICES PROCUREMENTS, 2015-2017

The objectives of Phase I of FX were to procure a Strategic Enterprise Advisory Services (SEAS) Vendor and an Independent Verification and Validation (IV&V) Vendor. Additional objectives of Phase I included operating an interim Project Management Office (PMO) using existing Agency resources in the Bureau of Medicaid Fiscal Agent Operations in advance of the SEAS Vendor and extending the current Fiscal Agent contract beyond the current end date of June 30, 2018 to ensure the continued operation of the FMMIS/DSS/FA during the FX transition period.

Strategic Enterprise Advisory Services (SEAS)

The Agency contracted with North Highland in 2017 to meet the first objective. The SEAS Vendor was tasked with providing the consulting expertise needed to develop the strategic plan for FX in accordance with the MITA Framework 3.0 and the CMS Standards and Conditions, develop and manage the FX Governance, manage a PMO for FX projects, develop data and technical standards, develop and maintain information and technical architecture documentation, and establish an enterprise data security plan. The SEAS Vendor was also tasked with providing strategic project portfolio management including assisting the Agency in developing Advanced Planning Documents (APDs) needed for requesting federal enhanced funding for FX projects. As Medicaid modules are developed, the SEAS Vendor will manage the Medicaid Enterprise Certification process and provide the Agency with early feedback from CMS that may impede certification. In sum, the SEAS Vendor provides the technical advisory expertise to identify solutions that meet current and future business needs of FX in an incremental and efficient way, and provides ongoing strategic, technical advisory, and programmatic services.

Independent Verification and Validation (IV&V)

The IV&V Vendor, NTT DATA State Health Consulting, LLC (formally Cognosante, LLC), was tasked with providing an independent and unbiased assessment of deliverables produced by FX vendors, including the SEAS Vendor. The IV&V Vendor assesses and reports on each FX project's

organization, planning, procurement, management, and technical solution development and implementation, and produces IV&V progress reports and related checklists required for CMS certification. IV&V services are required by federal regulation 45 CFR § 95.626 to represent the interests of CMS and are also required pursuant to the Florida Information Technology Project Management and Oversight Standards found in Florida Administrative Rule 60GG-1.001 through 60GG-1.009, Florida Administrative Code (F.A.C).

DXC Extension to July 2020

On April 25, 2018, CMS approved the Agency's request to renew the DXC Technology Fiscal Agent contract for two years through July 31, 2020, thereby completing the third objective of Phase I. The contract renewal included several self-service enhancements for the Medicaid operations at no cost and a turnover requirement for each component of the legacy FMMIS, as new FX modules are implemented. This extension was scheduled to terminate on July 31, 2020, unless renewed in accordance with section 287.057, Florida Statutes (F.S.).

PHASE II: FX INFRASTRUCTURE

The Phase I objectives helped establish the framework and discipline for the Agency to tackle the Phase II goal of building the foundation of modularity.

The objectives of Phase II included procurements of an Integration Services and Integration Platform (IS/IP) and an Enterprise Data Warehouse (EDW). As anticipated, the Agency released both ITNs in 2019. The Agency released the IS/IP ITN in January 2019 and executed the contract on November 14, 2019. The IS/IP Vendor provides the technical expertise to ensure the integrity and interoperability of FX by performing technical systems integration in coordination with multiple vendors providing the technology solutions. The IS/IP platform provides a standards-based integration platform to connect diverse applications and enable a common information exchange process between systems.

The Agency released the EDW ITN in July 2019; the selected vendor will provide data management, data warehousing, and data integration capabilities across systems and will replace the current Decision Support System/Data Warehouse (DSS/DW). The Agency is designing an EDW solution architected to provide a single source of truth for Agency data, greater information sharing, broader and easier access, enhanced data integration, increased security and privacy, and strengthened query and analytic capability by building a unified data repository for reporting and analytics.

Phase II has the potential to include an objective to integrate business and technical services and data from current Agency systems through the implemented integration platform and enterprise data warehouse. Agency business areas often operate with their own version of data and tools, business rules/policy, application systems, and strategies to share and reuse information with other business areas. Through the initial planning of FX, it was determined that the current data architecture is causing many data challenges as there is no single source of the truth as each Agency business area has its own data, and there are many challenges with how business areas share data

to perform day-to-day functions. For example, there are over 60 applications involved in Medicaid that use multiple data stores across the enterprise. As a result, Phase II could include activities to develop and implement interfaces to IS/IP from existing AHCA systems such as Enrollment Broker and others that are identified during IS/IP and EDW implementations. This opportunity only exists with the required budget to appropriate funds to these activities. The current requested level does not include these activities within the scope of Phase II.

Summaries of the infrastructure elements required in Phase II are included below:

Integration Services and Integration Platform (IS/IP)

IS/IP serves as the conduit, or interface, through which all information is requested and returned. It includes an Enterprise Service Bus, which controls information flow in and out of all modules. IS/IP's scope also contains a Business Rules Engine to help ensure all federal and state rules are accurately applied, with a Service Registry to maintain an inventory of services across all systems. IS/IP is coupled with the Master Person Index/Master Organization Index and Single Sign-On. FMMIS and the larger Florida Medicaid Enterprise currently rely heavily on point-to-point system integrations, flat file transfers, and multiple sign-on or authentication solutions. The Enterprise Service Bus in IS/IP will simplify and streamline technology components that will communicate with each other. Single sign-on will simplify user access and account provisioning at the Agency by managing authentication of users across multiple systems. The master person and organization index will present a consolidated master view of providers and recipients, reducing costly duplicative or invalid actions caused by redundant records.

Enterprise Data Warehouse (EDW)

It is critically important to have a data warehouse solution that allows the Agency to conduct complex analysis of program data for many aspects of Medicaid, from health outcome measurements to managed care rate setting. The Agency's EDW contract will include operational services and analytical tools to meet the Agency data requirements. The EDW will be a best-in-class data repository that, along with the enhanced analytical tools and operational services, including an Operational Data Store, will provide:

- A single source of truth to improve data quality, accuracy, and accessibility
- A data management solution for new modular business processing solutions
- Improved timeliness and consistency of data
- Improved predictive modeling and analytic data processing with holistic business unit and personal optimized data marts and tools
- Elimination of duplicated, inconsistent data and processing
- System innovation and simplified system implementation
- Improved data protection and privacy including authorizing and logging of data use
- Minimization of data conversion costs from future system replacements

PHASE III: FX FMMIS RESOLUTION

During the FY 2019-20 Legislative Session, the Agency was granted the option to extend the Fiscal Agent contract through December 2024. The objectives of Phase III were then focused on meeting the statutory deadline to transition from the current Fiscal Agent contracted system and services by December 2024. Phase III includes activities to procure modules to transform and improve the business processes that are currently occurring within the FMMIS, replacing this functionality with solutions that are interoperable with other systems within FX, and potentially within the larger Florida HHS Agency ecosystem. The Agency will complete these procurements using open source solutions, configurable COTS products, or other modular approaches that eliminate the need for custom development.

As Phase III: FX FMMIS Resolution is completed, the functions currently performed in the Fiscal Agent contract, the FMMIS, DSS, and some other Agency systems will be fully transitioned to modules that will provide greater efficiency and effectiveness in the administration of the Medicaid program. A visual depiction of the FX procurement strategy including the end of Phase II and all of Phase III is included below. **Figure 4: Phase III: FX FMMIS Resolution**, includes summaries of the modules required in Phase III to resolve FMMIS.

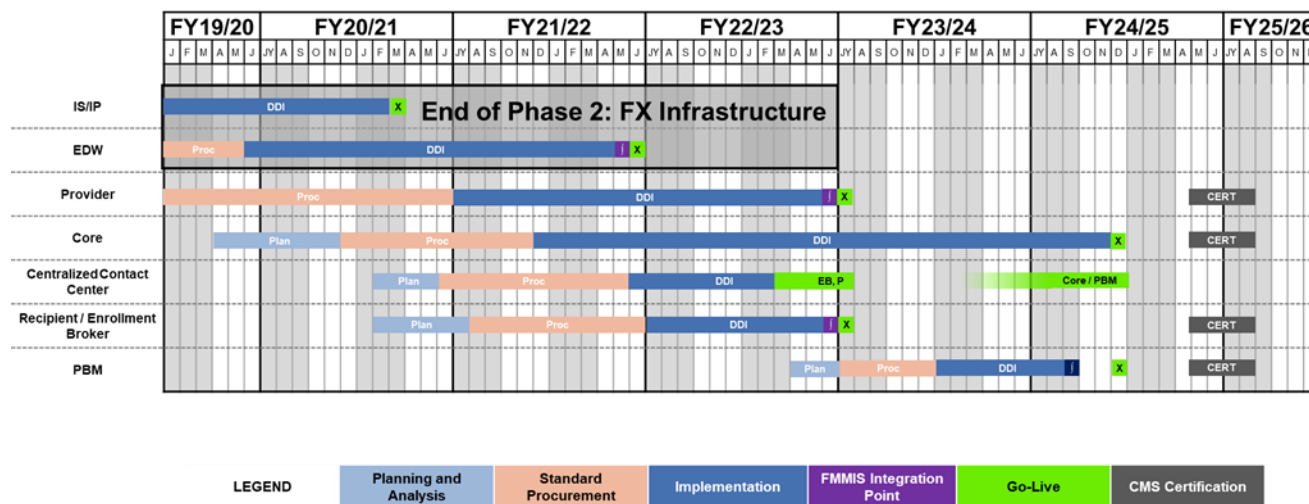


Figure 4: Phase III: FX FMMIS Resolution

Provider Management Module

The Provider Management Module is the next module to be procured. The business case was approved by FX Governance, allowing planning and procurement project activities to start in August 2019.

With the increased emphasis on provider enrollment and management resulting from the Affordable Care Act (ACA) and the Agency’s implementation of Statewide Medicaid Managed Care (SMMC), the Agency has a need to increase the technical maturity of the Provider

Management business process. The Agency will leverage the Master Person Index and Master Organization Index developed by the IS/IP Vendor in order to make technology, process, and policy improvements for provider identity reconciliation. Additionally, the provider management module will improve the provider experience and reduce the administrative burden for enrollment and credentialing. FX intends to streamline the provider enrollment process, resulting in an improved experience and faster provider enrollment in Medicaid.

The Agency expects the new FX provider management solution will integrate with other systems that use provider data, such as the Florida Department of Health practitioner licensure system, the Health Quality Assurance facility licensure system, and the Provider Background Screening Clearinghouse. However, interoperability is dependent on stakeholder prioritization, including that of the Governor, Legislature, Executive Leadership of AHCA, Executive Leadership of other sister agencies, and the appropriation of funds.

Core Module (Claims / Encounters / Enterprise Financial Management)

The Agency is evaluating the current core FMMIS functions that include claims transaction processing, banking and financial processing (including capitation payments for SMMC health plans), claims payments, and pharmacy claims payment. Core FMMIS functions also include reference file management for edits and audits, benefit plans, coverage rules, reimbursement rules, diagnosis codes, procedure codes, modifiers, diagnosis related group, revenue codes, and error codes. These functions are interconnected and are planned to be transitioned from the current FMMIS into a single Core module for integration with FX. As the name suggests, this module represents the most essential functionality required for Medicaid processing and involves the longest combined timeframe for planning, procurement, and implementation. Planning and analysis are slated to begin by Quarter 4 FY 2019-20 and all innovative options will be considered to accelerate the procurement and implementation of this critical component.

Centralized Contact Center

Current operations of the FMMIS and other Agency systems and operational activities includes multiple contact centers, vendors, and supporting software platforms. As a result, no unified record of Agency communications with different stakeholder groups is possible. Consequently, the user experience of the stakeholders is disjointed and confusing. In addition, the multi-vendor and multi-platform environment is resulting in redundant costs that could be handled more efficiently if consolidated. The Centralized Contact Center will include the systems and infrastructure to support inbound and outbound multi-channel communications between the Agency and its stakeholders across the breadth of FX. The Agency will consolidate communications and operational aspects of several current systems and vendors including the modules replacing the FMMIS / current Fiscal Agent contract and the Agency Recipient / Enrollment Broker module. This Centralized Contact Center will include the network, telephony, and systems used in contact management. It will support interactions by phone, email, chat, SMS text, social media, voice assistant, internal / external conference, physical mail, and in-person channels. Major components include unified contact distribution and routing, self-service interaction capabilities (e.g., interactive voice

response and chatbots), workforce management, quality assurance, contact recording and translation, multi-language support, and contact knowledge management.

Recipient/Enrollment Broker Module

The Enrollment Broker functionality currently includes the systems, contact center / platform, and operations that allow recipients to evaluate and select a health plan. This scope represents the largest element of the Agency's vision for a future Recipient module that will enhance and improve the experience of Medicaid recipients. The current Agency Enrollment Broker contract will exhaust its possible renewal and extension options in FY 2023-24, which is a constraint that is driving the planned timing for the Recipient/Enrollment Broker module. Other scope planned for this module include:

- Recipient management functions to maintain recipient information, grievances, appeals, communication, and interactions
- Population and recipient outreach functions to notify recipients about relevant changes or updates to health plans, their benefits, a provider, or other relevant information
- A portal to house required Recipient functionality and communications tools to support a unified and consistent Recipient user experience

Recipient communication may be generated by the Recipient/Enrollment Broker module but will leverage the Centralized Contact Center for efficiency.

Pharmacy Benefits Management Module

The Pharmacy Benefits Management (PBM) module performs the PBM functions required to replace these activities as they are included in the current FMMIS/Fiscal Agent contract. This module will perform financial and clinical services for the fee-for-service (FFS) Medicaid population including drug price negotiation with manufacturers. PBM also includes a system to process pharmacy claims and e-prescribing and integration with pharmacy point of sale systems, pharmacy fee collection, and pharmacy rate negotiation. PBM scope also contains prior authorization for certain required drugs. The future PBM vendor will be required to monitor prospective and retrospective drug utilization and oversee preferred drug lists (PDL). The PBM vendor will also provide operational staff to deliver information to providers, pharmacists, and recipients.

PHASE IV: REMAINING NON-FMMIS MODULES

The objective of Phase IV is to procure and implement the remaining non-FMMIS modules planned in FX that are necessary to accomplish the FX Vision of transforming ...the Medicaid Enterprise to provide the greatest quality, the best experience, and the highest value in healthcare.

Figure 5: Phase IV: Remaining Non-FMMIS Modules includes the non-FMMIS modules required to complete the transformation.

state agencies, which maintain information on the same entities, providers, and recipients. Streamlining this information into a single system will facilitate the availability of complete and comprehensive information for state agencies, entities, providers, and recipients. Existing case tracking systems will be retired as the information and business processes are migrated to the enterprise solution, thereby reducing costs and promoting sharing, and the reuse of technologies and systems, in accordance with CMS Standards and Conditions.

FY 2019-20 included budget for the implementation of a Legal Case Management solution that covers the automation of manual processes and a standardized file management solution for the Agency legal case management and tracking at a minimum. This solution may eventually be scalable over time to accommodate the larger enterprise case management goals described above. However, if the Legal Case Management solution is determined to not meet the Agency's enterprise needs, an enterprise solution procurement will begin in FY 2024-25 as outlined on the Phase IV visual depiction above.

Contractor Management Module

A large volume of Agency work depends heavily on the work and management of contractors and partners. The Contract Management module will include a system that manages the Agency's contract life cycle from procurement through contract termination. The system will centralize all contract information, provide an in-depth understanding of contract terms and compliance requirements, and provide customized stakeholder views to help manage compliance and support performance management, accountability, transparency, and automated imposition and collection of liquidated damages.

Currently, the Agency relies on the Contract Administration Tracking System (CATS) for some of these activities and for the transfer of data to the Fraud and Abuse Case Tracking System (FACTS). At a future date, the CATS system will be evaluated for its potential as a long-term solution.

The Contractor Management module systems and business process operations dedicated to performance management are similarly transformational to the Plan Management module discussed above. This module will radically improve the Agency's ability to manage contract performance on the body of work dependent on contractors meeting their service-level agreements and performance standards. The Contractor Management module system will develop and automate the reports and other mechanisms that the Agency will use to track activity and effectiveness at all levels of monitoring. Business intelligence analysis (i.e., historical, current, and predictive views of business operations) will measure the performance of contractor activities and programs against widely accepted outcome metrics (e.g., Consumer Assessment of Healthcare Providers and Systems (CAHPS) and Healthcare Effectiveness Data and Information Set (HEDIS) measures). The solution will leverage the EDW tools and infrastructure as appropriate.

3.1.1 SYSTEM GOALS AND OBJECTIVES

FX Will Accomplish Agency Goals for the Florida MES Efficiently and Cost-Effectively

FX is defined as the transformation of the business, data, services, technical processes, and systems necessary for the administration of the Florida Medicaid Program. The FMMIS has historically been the central system within the Florida Medicaid Enterprise, functioning as the single, integrated system of claims processing and information retrieval. As the Medicaid program has grown more complex, the systems needed to support the Florida Medicaid Enterprise have grown in number and complexity. The current Florida Medicaid Enterprise includes the FMMIS as well as separate systems that function to support Florida Medicaid and the Agency. Such Agency systems include, but are not limited to, the enrollment broker system, third-party liability, pharmacy benefits management, fraud and abuse case tracking, prior authorization, home health electronic visit verification, provider data management system, and Health Quality Assurance licensure systems. The Florida Medicaid Enterprise also includes interconnections and touchpoints with systems that reside outside the Agency such as systems hosted by the Department of Children and Families, Department of Health including Vital Statistics, Department of Elder Affairs, Agency for Persons with Disabilities, Florida Healthy Kids Corporation, Department of Financial Services, Florida Department of Law Enforcement, and Department of Juvenile Justice.

The FX procurement strategy proposed a phased approach to replace the current functions of the FMMIS based on the CMS Standards and Conditions to ultimately transition to an interoperable and unified Medicaid Enterprise where individual processes, modules, sub-systems, and systems work together to support the Medicaid program. This approach is intended to provide the most efficient and cost-effective long-term solution for FX while complying with federal regulations, achieving federal certification, and obtaining enhanced federal funding.

Summary of the FX Vision, Guiding Principles, and Strategic Priorities

Agency executives developed the FX Vision by tying the FX strategy to the overall mission, vision, and goals of the Agency.

The Agency's Mission is to *Drive transformation of the health care system to increase accountability through improved health outcomes with efficient and effective use of taxpayer resources.*

The Agency's Vision and long-range goals support the Agency's Mission. According to the 2019 Long-Range Program Plan the Agency's Vision is *A high quality, safe and affordable health care delivery system for all Floridians.* The Agency's long-range goals, as laid out in its Long-Range Program Plan, also support the Agency's Mission and are as follows:

- To operate an efficient and effective government
- To reduce or eliminate waste, fraud, and abuse
- To ensure a stronger health care delivery system by getting the incentives in Medicaid right: allowing Florida Medicaid enrollees to choose a health plan based on quality and customer service to ensure Florida enrollees receive the care they need and deserve

Agency executives collaborated with the SEAS Vendor to create the FX Vision and the supporting Guiding Principles and Strategic Priorities during a Strategic Visioning Session held on December 13, 2017. The Vision, Guiding Principles, and Strategic Priorities were later confirmed and revised as needed during the strategic refresh effort that included another Strategic Visioning Session on December 13, 2019. During these sessions, the SEAS Vendor and Agency executives used the Agency's Mission, Vision, and Goals as guides to create the FX Vision and Guiding Principles. As a result, the FX Vision and Guiding Principles support the Agency's Mission, Vision, and Goals to effectively guide the Agency's investment decisions during the transition to a modular environment.

The Agency's FX Vision is to *Transform the Medicaid Enterprise to provide the greatest quality, the best experience, and the highest value in healthcare.*

The Agency's FX Guiding Principles must be adhered to if the FX Vision is to be achieved. They therefore support the FX Vision and are as follows:

- Enable high-quality and accessible data
- Improve healthcare outcomes
- Reduce complexity
- Use evidenced-based decision-making
- Improve integration with partners
- Improve provider and recipient experience
- Provide good stewardship of Medicaid funds
- Enable holistic decision-making rather than short-term focus

The FX Guiding Principles also support CMS' Medicaid Information Technology Architecture (MITA) Goals and Objectives. A link to the 2019 MITA SSA can be found in Appendix A.

The FX Guiding Principles are, in turn, supported by strategic priorities which define the areas of practical importance to achieve the FX Vision. The twelve FX Strategic Priorities are covered below. The first five are the highest priority and most influential in terms of influencing FX decision-making.

1. Reduce risk of integration and cost associated with legacy FMMIS by accelerating procurements to resolve / replace its functionality
2. Improve provider experience by streamlining credentialing and licensing, and developing a Master Person Index, and a Master Organization Index
3. Prioritize high-quality accessible data, analytics, and reporting
4. Prioritize joint efficiencies with interoperability within AHCA
5. Strategically leverage efficient procurement vehicles where possible
6. Maximize staff efficiency
7. Prioritize renegotiating and improving both functionality and technology for large (non-FMMIS) system contracts
8. Prioritize joint efficiencies with interoperability across other HHS agencies

9. Improve recipient visibility and experience through consolidated portal and contact center functionality where possible
10. Maximize accountability for vendor performance
11. Align to CMS modularity to streamline system transformation and modernization
12. Reduce impacts on Agency and staff

The Agency’s transformation plan translates the Strategic Priorities into tangible effects on stakeholder roles and data exchanges. The strategy articulation map below, **Figure 6: FX Strategy Articulation Map**, highlights the key focus areas for the FX Program and the overarching goals that FX will achieve.

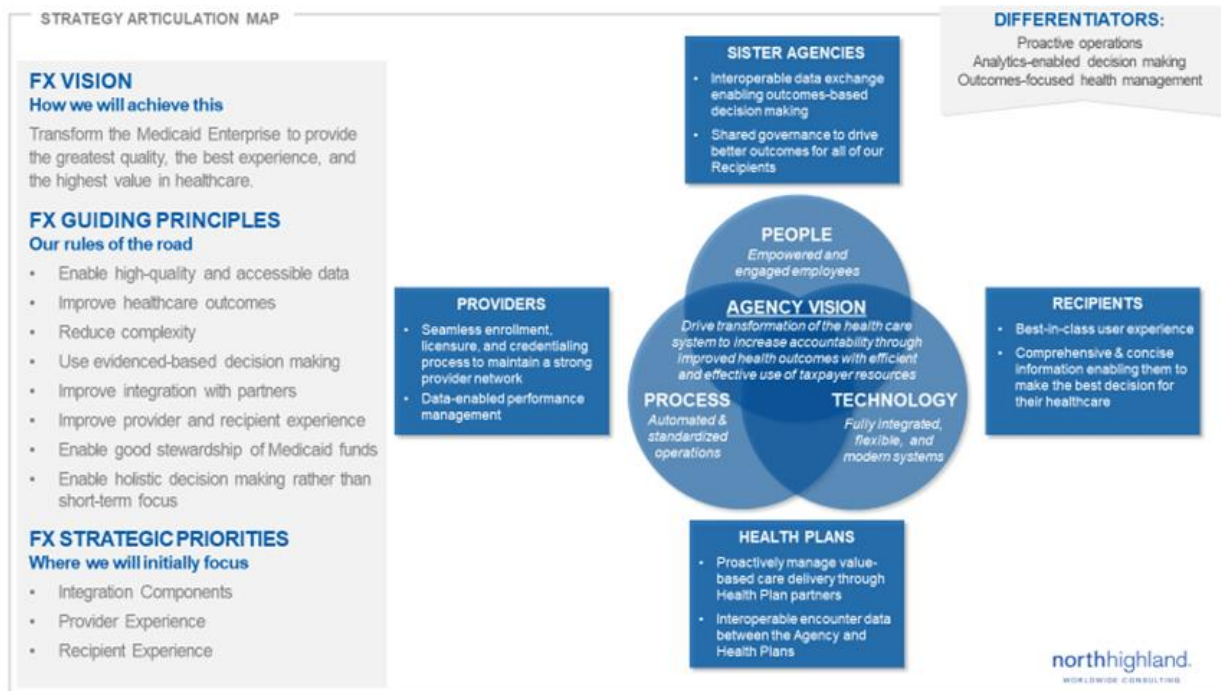


Figure 6: FX Strategy Articulation Map

The CMS Modularity Standard requires the Agency to move away from the current large, highly complex, and highly customized MMIS enterprise systems and towards smaller, less customized modules. To enable this modular environment, the Agency must deploy standards-based data exchange and information architecture to enable systems to communicate effectively with one another in an interchangeable manner. This will enable the Agency to improve consistency around system functionality and service by easily modifying systems independently of the rest of the enterprise.

3.2 PROPOSED SYSTEM

The FX transformation program proposes a phased approach to replace the current functions of the MMIS based on the CMS Standards and Conditions to ultimately transition to an interoperable and unified Medicaid Enterprise where individual processes, modules, sub-systems, and systems

work together to support the Medicaid program. The FX transformation program will replace large, core aspects of the existing MMIS and fundamentally change Medicaid business processes for the better across multiple stakeholder groups encompassing recipients, providers, and Agency staff.

The recommended business solution for Phase I of the FX transformation program was to procure a SEAS Vendor to obtain the expertise needed to develop the framework for the Medicaid Enterprise in accordance with the CMS Standards and Conditions, including MITA 3.0, and facilitate the interoperability of business and technical services across the Medicaid Enterprise. The scope of work for the SEAS Vendor includes strategic, programmatic, and technical advisory services to support the phased approach to the FX transformation program. The Agency procured the SEAS Vendor, and the contract was executed in September 2017. The Phase II business solution for the FX transformation program includes IS/IP and EDW procurements.

During the FY 2019-20 Legislative Session, the Agency was granted the option to extend the Fiscal Agent contract through December 2024. The objectives of Phase III were then focused on meeting the statutory deadline to transition from the current Fiscal Agent contracted system and services by December 2024. Phase III includes activities to procure modules to transform and improve the business processes that are currently occurring within the FMMIS, replacing this functionality with solutions that are interoperable with other systems within FX, and potentially within the larger Florida HHS agency ecosystem. The Agency will complete these procurements using open source solutions, configurable COTS products, or other modular approaches that eliminate the need for custom development.

The objective of Phase IV is to procure and implement the remaining non-FMMIS modules planned in FX that are necessary to accomplish the FX Vision of transforming ...the Medicaid Enterprise to provide the greatest quality, the best experience, and the highest value in healthcare.

Figure 6: FX Strategy Articulation Transformation depicts the Medicaid Enterprise future state modular environment.

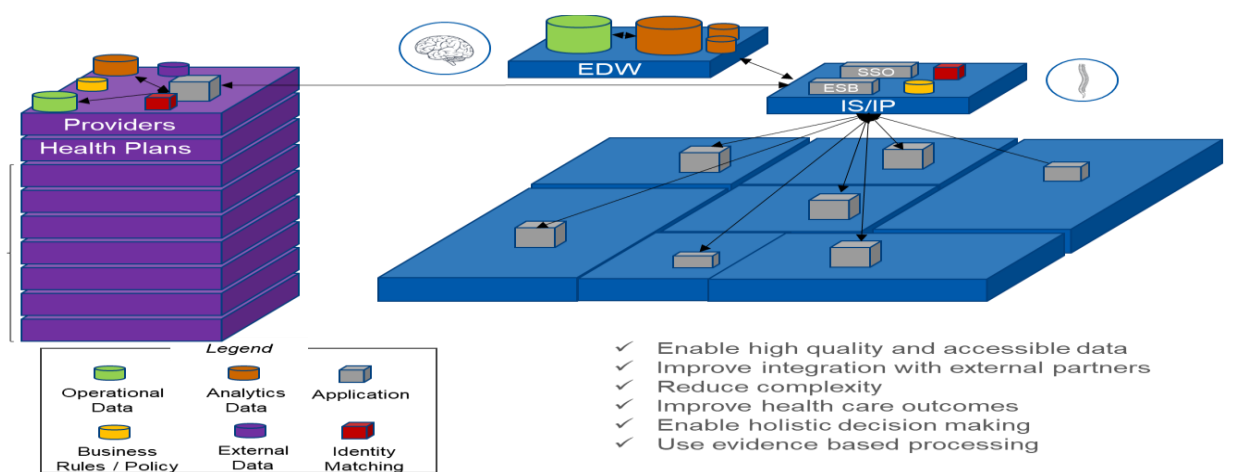


Figure 7: FX Modular Transformation

3.2.1 SYSTEM SCOPE

The proposed technical solution is to procure modules to replace business processes within the MMIS that are interoperable with other systems within the FX transformation program, using open source solutions, COTS products, or other modular approaches that reduce the need for custom development. Proposed solutions include the EDW and IS/IP, and modular procurements for Provider Management, Claims Processing, Encounter Processing, Financial Management, Centralized Contact Center, Recipient Management, Pharmacy Benefits Management, Plan Management, Third Party Liability, Case Management, and Contractor Management.

The proposed solution supports the FX Data Management Vision which emphasizes six primary strategies that align with the overall FX strategic priorities:

- Improve data quality by operating from a single source of policy truth
- Evolve core processing with data validation at the point of business event data collection
- Provide seamless access to a real-time, 360-degree view of recipient and provider information
- Decouple data from proprietary systems and application stores
- Operate with business area and persona optimized data marts and data analysis tools
- Prepare to collect and manage recipient and provider experience and outcome data

3.2.2 BUSINESS PROCESSES SUPPORTED

The project was initially conceived as a MMIS replacement. However, through the strategic planning process the Agency determined that the Medicaid Enterprise required a comprehensive transformation to fulfill its mission to *drive transformation of the health care system to increase accountability through improved health outcomes with efficient and effective use of taxpayer resources* while meeting evolving federal requirements and standards and responding to a changing healthcare landscape. The FX transformation program is not only transformative for the Agency, but will improve how FX business process are conducted, thereby affecting Agency staff, other agencies, providers, plans, and recipients.

Through the 2014 State Self-Assessment (SS-A) development, the Agency, along with consultants procured to assist with the process, conducted Requirement Analysis and Development sessions to completely describe the business process needs for the FX transformation program. The 2018 and 2019 SS-A update focused on the business processes associated with the near-term strategic priorities of the EDW, IS/IP, and Provider Services, which drive progress towards the Agency's goals of improving data quality, promoting modularity, and enhancing provider experience. While the SS-A captures high-level business process requirements, solicitation documents for module procurements and other projects will define the detailed requirements. **Table 1: Supported Business Processes** shows the business processes selected for reassessment in 2018 and 2019.

ENTERPRISE DATA WAREHOUSE	PROVIDER MODULE
<ul style="list-style-type: none"> ▪ BR03 – Manage Business Relationship Information ▪ CM02 – Manage Case Information ▪ CO01 – Manage Contractor Information ▪ FM06 – Manage Accounts Receivable Information ▪ FM13 – Manage Accounts Payable Information ▪ FM17 – Manage Budget Information ▪ ME01 – Manage Member Information ▪ OM28 – Manage Data ▪ OM29 – Process Encounters ▪ PE03 – Manage Compliance Incident Information ▪ PL01 – Develop Agency Goals and Objectives ▪ PL04 – Manage Health Plan Information ▪ PL06 – Manage Health Benefit Information ▪ PL07 – Managed Reference Information ▪ PM01 – Manage Provider Information 	<ul style="list-style-type: none"> ▪ EE05 – Determine Provider Eligibility ▪ EE06 – Enroll Provider ▪ EE07 – Disenroll Provider ▪ EE08 – Inquire Provider Information ▪ PM01 – Manage Provider Information ▪ PM02 – Manage Provider Communication ▪ PM03 – Perform Provider Outreach ▪ PM07 – Manage Provider Grievances and Appeals ▪ PM08 – Terminate Provider

Table 1: Supported Business Processes

3.2.3 HIGH LEVEL FUNCTIONAL REQUIREMENTS

The Agency is pursuing a transformative approach to become a data-centric organization. Data has always been critical to the work the Agency, health plans, providers, and external organizations perform. The Agency is changing its treatment of data as an asset to the healthcare ecosystem. Historically, data was a component embedded within a specific system focused on specific business processes. Applications and data were tightly linked, often as isolated islands specific to a business unit or business process. When the Agency replaced applications or the vendors providing processing services, the process to convert or migrate data for use in a new system was complex and difficult.

The approach AHCA is pursuing in its vision is to change the relationship between data and systems. The Agency seeks to make healthcare data a permanent asset that is managed and retained regardless of systems or organizations using the data. The centralization of this important asset will provide a single source for consistent data validation and application of business policy. With this approach, the Agency expects better data quality, expanded use throughout the healthcare ecosystem, and increased innovation from stakeholders and the vendor community to improve health care for all Floridians.

The EDW vision recognizes that there are currently—and will likely be ongoing—technical and organizational boundaries requiring data be kept in multiple data stores. The Agency is implementing an IS/IP solution to allow information to be stored in multiple data stores in a manner consistent with the Agency’s vision. The IS/IP solution will provide near real-time connectivity to external data sources allowing redundant information to be accessed and presented in a cohesive view in near real-time. The use of integration services to assemble and consolidate data from

multiple sources will help the Agency achieve some of the benefits of its vision as the operational data store grows, and duplicated data is reduced. Over time as operational data is decoupled from application systems, the expectation is the IS/IP platform will integrate fewer and fewer sources (only those external to the operational data store).

Industry technology trends aligned with the EDW vision (e.g., the use of Blockchain) anticipate that eventually all stakeholders in the healthcare ecosystem will contribute and access information from a secure single source. Therefore, the EDW vision contemplates that health plans, providers, and external organizations may ultimately operate from the single source of truth thus reducing internal duplication and processing delays.

The EDW system, as currently envisioned, is comprised of the Operational Data Store (ODS) and Content Management (CM) Repository, the Analytic Data Store, the Persona Optimized Analytics and Reporting (POAR) component, and Specialized Data Stores (SDS). Combined, these components will address the challenges presented by the MES Current State.

By providing a single location for all transactional data and digital content retained by the Agency, the ODS and CM Repository strives to rectify the data inconsistencies and multiple versions of *truth* present in the current state.

The Analytic Data Store is comprised of the Reporting Data Store (RDS), the Analytics Data Store, and various data marts. These components will provide rapid and timely access to high quality data captured from the ODS via well-defined replication and Extract, Transform, and Load (ETL) processes.

The POAR component will provide a unified set of tools intended to create consistent analytical, modeling, and reporting processes thereby increasing confidence in the reports and models produced by and for the Agency.

The SDS rounds out the EDW solution by providing the capability to efficiently produce data structures and data stores to meet specialized needs of the Agency (e.g., data requests from external entities such as other state agencies, academic institutions, media outlets).

Together, these components form a cohesive and effective response to the Agency's need for reliable, accurate, and timely data while also addressing the need for dependable analytics and predictive modeling and forecasting.

The Provider Management Module (PMM) is the next module to be procured. The business case was approved by FX Governance, allowing planning and procurement project activities to start in August 2019.

With the increased emphasis on provider enrollment and management resulting from the Affordable Care Act (ACA) and the Agency's implementation of Statewide Medicaid Managed Care (SMMC), the Agency has a need to increase the technical maturity of the Provider Management business process. The Agency will leverage the Master Person Index and Master

Organization Index developed by the IS/IP Vendor in order to make technology, process, and policy improvements for provider identity reconciliation. Additionally, the Provider Management module will improve the provider experience and reduce the administrative burden for enrollment and credentialing. FX intends to streamline the provider licensure and enrollment process, resulting in an improved experience and faster provider enrollment in Medicaid.

The goal of the recommended PMM alternative is to operate, manage, control, and configure provider management, including functionality for online licensure and enrollment (both initial and renewal) through a single, centralized portal. By integrating other Medicaid Enterprise agencies into its functionality, the recommended PMM alternative is also aligned to the guidance from CMS on system interoperability. Key functions and elements of the recommended PMM alternative include:

- Consolidated licensure (professional and facility), Medicaid enrollment, and plan credentialing into a concurrent process
- Automated account management updates triggered through electronic interfaces or initiated by the provider, such as change of address, change of ownership, hours of operations, name change, and network rosters
- Workflow assignment and efficient business processes for Agency staff reviews and approvals
- Application tracking to clearly communicate the status to pending providers
- Quality data and analytics supported by IS/IP and EDW to assist staff in monitoring all aspects of the provider life cycle
- Ability to decommission current Fiscal Agent provider functionality

The Agency intends that the new FX provider management solution will integrate with other systems that use provider data, such as the Florida Department of Health practitioner licensure system, the Health Quality Assurance facility licensure system, and the Provider Background Screening Clearinghouse.

Figure 6: FX Strategy Articulation Model depicts the vision and conceptual design for the future state of the Medicaid Enterprise.

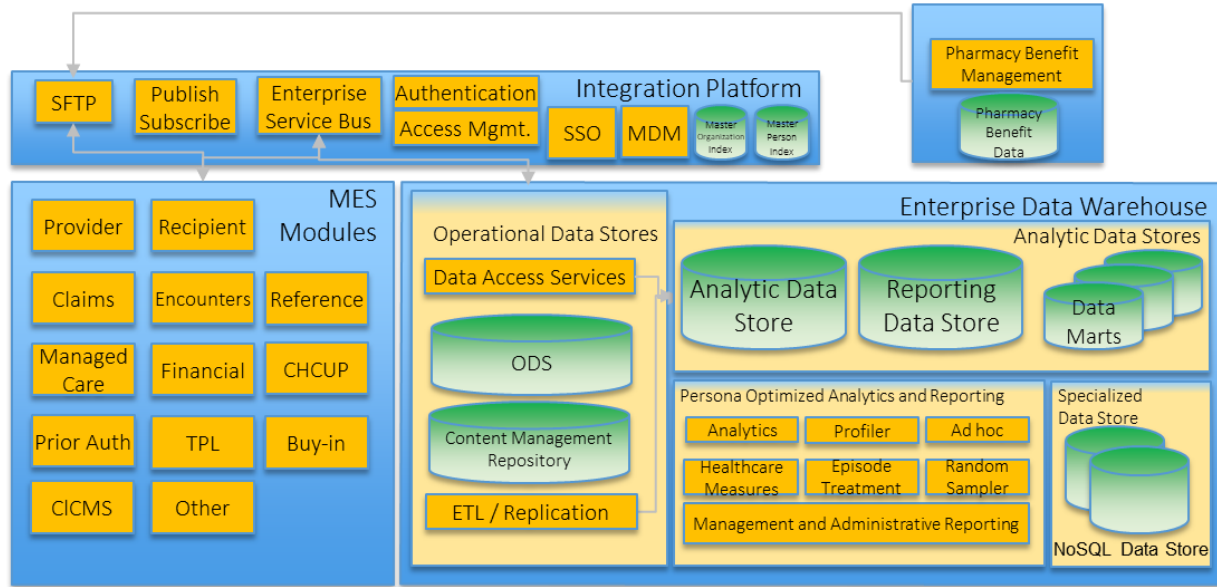


Figure 8: FX Transformation Model

SECTION 4 SCENARIOS ANALYSIS

The Agency's approach focuses first on building the foundation for transformation through procurement of an IS/IP vendor and EDW services. The IS/IP and EDW procurements power the health of the Agency to live in a data driven healthcare ecosystem.

Figure 6: FX Strategy Articulation Foundation depicts the functions of the foundational IS/IP and EDW procurements.

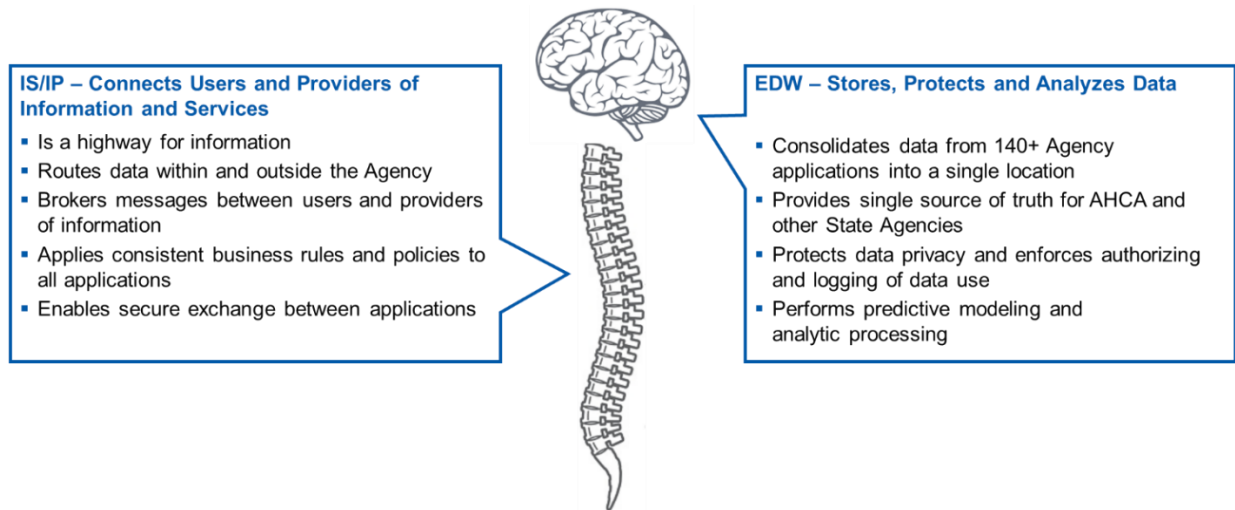


Figure 9: FX Transformation Foundation

The new IS/IP solution will enable people and systems within and outside the Agency to operate and act with the same information to accelerate service delivery. The integration platform consists of several components enabling new and existing systems to access and reuse data and processing across organization and system boundaries.

- Enterprise Service Bus - Validates, authorizes, and connects requestors and providers of data and processing services across the ecosystem
- Master Person/Organization Index - Links master records about a person or organization within or across systems so processing considers all relevant information
- Master User Interface - Provides pages to view and explore available information about a recipient, provider, or organization
- Single Sign-On - Provides internal and external users secure access to applications using a single id
- Enterprise Rules Engine - A repository and processing engine to make processing decisions (e.g., enrollment, pre-authorization, claim approval)
- Publish Subscribe Alerting - Allows systems to communicate information and events that are automatically shared with other organizations or systems

The EDW system will allow the Agency to become a data centric organization and improve data integrity and accuracy. The components of the EDW solution decouple systems and data to make healthcare data available and consistent throughout the ecosystem.

- Operational Data Store – Single source of truth for all transactional information collected and used by systems
- Operational Data Services – Service that systems use to access operational data; standardizes authentication, logging, access controls, and usage accounting
- Enterprise Data Warehouse – Data store optimized for analytical processing
- Reporting Data Store Services – Data store for dashboards, reports, and ad hoc users needing analytics of real time or near real time information
- Content Management Store – Store for specialized content types (e.g., documents, images, reports, blueprints, etc.)
- Data Marts – Data stores organized for analytical processing specific to a business unit or persona
- Specialized Data Marts – Data stores optimized for specialized types of analysis or special project
- Analytic Tools – Tools to perform reporting, analysis, predictive modeling, and other types of analysis on health-related data

The first module procured will be the Provider Management Module (PMM). The preferred solution for a PMM aims to create a module or cohort of modules for Medicaid provider management allowing for concurrent processing of licensure, enrollment, and plan credentialing activities for both initial licensure and enrollment as well as renewals.

The PMM will also eliminate siloed activities that act as predecessors for additional onboarding tasks. Furthermore, the need for providers to interact and react to requests from multiple entities will be alleviated. Time delays in the onboarding process will be decreased through a single request for required documentation, concurrent processing activities, and data sharing among agencies and AHCA divisions.

In addition to provider licensure and enrollment activities, the desired functions of PMM include provider account management processes such as name change, address change, change of ownership (CHOW), and specialty addition or change.

Initial identified features of a desirable PMM include:

- Combined Licensure, Medicaid Enrollment, and Credentialing (initial and renewal)
 - › A single online portal with single sign-on capabilities to address all licensure, enrollment, and credentialing activities across agencies and AHCA divisions.

- › Provider-created user account and profile for future portal sign-on and authentication.
- › Real-time status for provider applications with adequate information and instructions to address the provider's needs.
- › Enhanced self-help features (e.g., implement provider self-service channels (web portal, Interactive Voice Response (IVR), mobile app, chat bots) to reduce contact center calls and emails) to assist providers in navigating through the enrollment process.
- › Secure online mailbox to inform providers of necessary action or disposition.
- › A single data source supported by IS/IP and EDW to be used and shared among agencies and AHCA divisions to limit the need for redundant information to be supplied by the provider.
- › Data to be collected electronically from originating sources through data agreements without the need for provider intervention. For example, if the Division of Health Quality Assurance (HQA) receives the results of a background screening, that information will be transmitted to Medicaid enrollment without the provider having to upload the document or the automation of Medicare Disqualifications to remove manual steps at Medicaid Program Integrity to apply Provider Restrictions.
- › Automated edits will be built into the portal to enhance the quality of data upon submission.
- › Real-time validation will enable the provider to immediately rectify any omissions or errors; the portal will not permit an incomplete or incorrect submission.
- › Validation of checklist items reviewed in the portal prior to submission for immediate feedback.
- › A single provider application regardless of the number of service locations.
- › A single credentialing source utilized by all plans (current provision in Managed Medical Assistance (MMA) contracts).
- › Streamlined renewal capabilities for provider reenrollment utilizing the electronic collection of data by the Agency without the need for provider intervention.
- Account Management
 - › Portal capability to act as a conduit for a unified change reporting site that will automatically disseminate the change to all appropriate entities and plans.
 - › Portal capability to collect licensure and renewal fees, fines, sanctions, and other monies owed.

- Communications
 - › Communication with providers in plain language that is clear and concise.
 - › Centralized correspondence tracking, including complaints.
 - › Notification mechanism to alert the provider community of new information.
- Performance Management
 - › Real-time or near real-time dashboard metrics to monitor all provider related processes.
 - › Quality and process indicators should be embedded into workflows for early detection and notification of issues.
 - › Enhanced data analytics supported by IS/IP and EDW to monitor all aspects of the provider life cycle, in addition to, network adequacy by provider type, location, facility, or plan affiliation.
- Workflow and Assignment Management
 - › Creation of dedicated work queues and assignment to specific user groups to complete tasks; assignment to the appropriate queue based on business rules that could include status, priority, task, and availability.
 - › Creation of Service Level Agreements (SLAs) that will define the acceptable timeframe and quality expectations for each stage of the process.
 - › Tracking and reporting on all relevant tasks throughout the life cycle, including tasks completed by Field Office staff, such as complaints and claims inquiries.
- Customer Care
 - › Implement provider self-service channels (web, IVR, mobile app, chat bots) to reduce contact center calls and emails.
 - › Future capabilities to enrich the view of the provider and avoid redundancies as program needs change allowing for reuse and leveraging.

The Agency will leverage the Strategic Project Portfolio Management Plan to identify future FX projects or modules. The Strategic Project Portfolio Management Plan is used for identifying, categorizing, evaluating, and selecting outcome-driven FX projects. This is a phase-gate project selection and approval process meaning that entry and exit criteria are considered in each phase with approval through FX Governance. A project must meet the criteria of a given phase to advance to the next phase. This process integrates with the Enterprise Systems Governance Plan and the MITA business areas. For the MES maturity efforts, outcomes are essential. The outcome model in the plan defines programmatic and operational outcome categories to evaluate projects.

- Programmatic outcomes focus on the strategic mission which are *big picture* items such as improve healthcare outcomes, reduce complexity, and improve provider and recipient experience.
- Operational outcomes are those that focus on achieving desired operational objectives such as the costs of administering a program, technology costs, staff costs, compliance with regulations and law, reduction of data silos, improved data quality, and analytics for operational efficiencies.

A way to improve outcomes is by implementing projects that improve program operations. Therefore, the portfolio management approach will show and select projects with desired outcomes aligned to the Enterprise Systems Strategic Plan. To maximize outcome improvements, the approach is to pursue projects in the right sequence using an evaluation and phase-gate process to categorize, evaluate, and select projects that improve outcomes.

As the Agency continues to execute its Enterprise Systems Strategic Plan, the process will evaluate potential projects against the strategic guiding principles and desired outcomes. This evaluation against the desired outcomes model scores potential projects in the portfolio. **Figure 10: Project Portfolio Management** depicts the stages and gate reviews of the process.

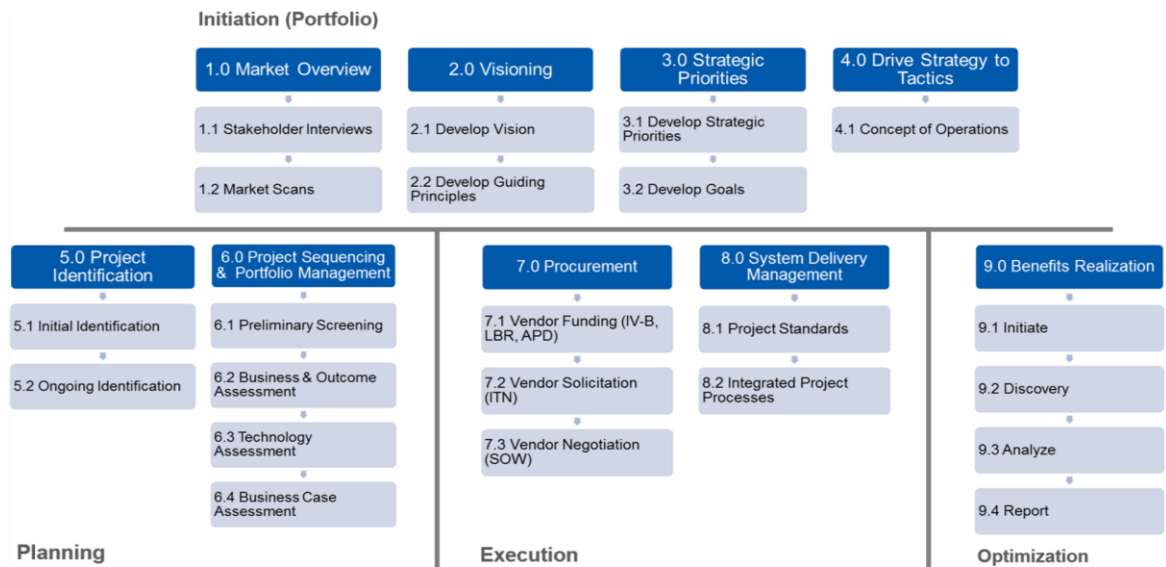


Figure 10: Project Portfolio Management

The Project Gating Process helps the Agency efficiently evaluate and prioritize ideas and potential projects/modules named by subject matter experts and stakeholders. The intake and evaluation of potential project investments occur using a gated evaluation process.

The overall purpose of the phase gates is to:

- Support preliminary project assessments to gauge alignment with the future state FX strategy, goals, guiding principles, policies, and standards

- Develop a project score and preliminary assessment of the impact to the business and technical architecture
- Identify other project and stakeholder dependencies and intersections
- Identify implementation risks and estimates associated with each project
- Identify initial architecture assurance needs indicated by the complexity profile of the project

Key Considerations:

- Ensure the projects, modules, and services required to deliver the business imperatives are identified and validated with the Agency and FX strategic priorities
- Highlight opportunities for re-use
- Look to highlight any cross-capability and cross-release issues
- Since each project has a different profile, size and scope gates need to be flexible, scalable, and adaptable
- A project may not fully align with the existing business or technical architecture, but may have a large business value and should therefore be considered for additional evaluation

Through the Portfolio Management process, future projects/modules will be evaluated for consideration. Business user scenarios will be identified through the Project Sequencing and Portfolio Management phase when assessment of business cases and outcomes are evaluated. As the process matures and projects are selected for execution, updates will be made to the MMIS Con Ops to capture additional transformation scenarios. Additional user scenarios should be developed during use case or user story elaboration.

Future potential business user scenarios include but are not limited to:

- Separating claims and encounter processing
- Becoming the gateway to public sector social determinant of health data
- Enabling integrated health and human service delivery
- One-stop provider licensing enrollment and regulation
- Enabling coordinated communications for recipient and provider communications
- Real time policy-based validation of transactions prior to submission
- Supporting hybrid vertical and horizontal health care service delivery

- Recipient engagement in their own wellness
- Recipient engagement in validation and verification of service delivery
- Improving and automating capture and analysis of provider and recipient experience metrics
- Using telemedicine to expand accessibility and reduce disruption when recipients move or relocate

SECTION 5 FACTORS INFLUENCING TECHNICAL DESIGN

5.1 RELEVANT STANDARDS

A technology standard is an established norm or requirement for technical systems. Standards are usually a formal document that establishes uniform engineering or technical criteria, methods, processes, and practices. The Technology Standards Reference Guide (TSRG) is a collection of technology standards applicable to the administration and operation of the enterprise and the future state enterprise. A comprehensive list of the Technology Standards identified for this project is located in [Appendix C](#).



Figure 11: TSRG Standards Hierarchy Example

Figure 11: TSRG Standards Hierarchy Example shows the types of organizations that are sources of relevant technology standards. Often standards of different organizations are aligned and consistent. Higher-level organizations may adopt lower-level standards or provide guidance that is more specific to the enterprise, organization, or system. In some cases, standards may conflict, or an organization may provide guidance that certain standards are waived or not applicable. The TSRG seeks to help stakeholders understand not only the universe of applicable standards, but also provides a framework and guidance to prioritize and resolve potential conflicting standards.

5.2 ASSUMPTIONS, DEPENDENCIES, AND CONSTRAINTS

The strategic plan and SS-A address the unique business requirements of the FX transformation program, including standards that affect the range of reasonable technical alternatives. On an enterprise level and on an individual project-by-project level, successful implementation of the technical, policy, and process alternatives identified through the project is contingent on assumptions and subject to constraints.

For the purposes of the project, assumptions are circumstances and events that need to occur for the project to be successful but are outside the total control of the project team. The following assumptions and constraints are identified:

- Agency and Vendor staff and other project stakeholders will be available and actively participate in the project activities and will respond to requests promptly
- Solicitations will result in the timely onboarding of the planned project consulting teams with minimal impact to the master project schedule critical path items
- The Agency will leverage alternative procurement approaches to accelerate the procurement and onboarding of vendors
- The FX governance structure will provide timely decision-making and project guidance to facilitate an integrated approach to the prioritization of time, resources, and budget across all Agency initiatives currently in progress and for any new initiatives over the life of the project
- MMIS Core Modules will use multi-layered application architecture in accordance with guidance provided by CMS
- Solutions must comply with federal and state security requirements to safeguard data and systems
- CMS Standards and Conditions and must be met by FX solutions
- MMIS activities will be ongoing during the FX transition; services to recipients must continue to be delivered
- Buy-in is needed from external stakeholders such as the State Legislature, partner state agencies, providers, and members
- Business processes may need to be re-engineered to align with change enabled by the future MMIS
- Competitive and innovative vendors must be ready and able to support modularity
- Adherence to the following interoperability application design principles is required:
 - › Standardized Contract – Expresses purpose, capability, and interface content quality to assure appropriate modularity and granularity
 - › Loose Coupling – Contains dependencies between the contract, deployment, and customer
 - › Abstraction – Hides as much of the details of the service to preserve loose coupling

- › Reusability – Positions services as enterprise resources with agnostic function content
 - › Autonomy – Design of the service logic and realization of environment impact reliability
 - › Statelessness – Managing excessive state information can compromise availability
 - › Discoverability – Avoid the accidental creation of redundant service or services that implement redundant logic
 - › Composability – Complex service composition places demands on service design
- Existing MMIS portals are developed and owned by different vendors that may use different technology stacks, style guides, data stores, and Application Programming Interfaces (APIs)
 - Updating all MMIS portals to have a unified user interface may not be possible without altering source code of vendor portals
 - The state budget process requires a lead time of 12 to 18 months from the time funding is requested until funds can be accessed
 - Legislative mandate to complete FMMIS related transition activities before December 31, 2024
 - The continued operations of the MMIS/DSS and Fiscal Agent are contingent upon execution of a contract extension beyond the current expiration date
 - Retire and replace scenarios must carefully consider current contract terms and scopes of work
 - Change in administration at the national and state level may impact funding, programs, and guidance
 - Standards are not consistently used when exchanging data with external agencies and contractors
 - To support a multi-year MMIS procurement and implementation, the Agency must address limited resource capacity and identify and dedicate resources with the necessary skill sets to the effort. Additionally, availability of state resources is critical for requirements and testing, while recognizing that data conversion is consistently the biggest time and resource consuming challenge. Multiple and overlapping implementations are taxing on state technical staff, so have a plan to adjust state resources as needed

- The completion of the implementation of the FX modular components, and Fiscal Agent operations, is contingent upon certification by CMS
- The Florida procurement process is a constraint relative to the overall project schedule
- The FX transformation program includes business processes and data transfers with outside agencies

5.3 AGENCY GOALS AND OBJECTIVES

Agency executives collaborated with the SEAS Vendor to create the FX Vision and supporting Guiding Principles during a Strategic Visioning Session held on December 13, 2017. During this session, the SEAS Vendor and Agency executives used the Agency's Mission, Vision, and Goals as guides to create the FX Vision and Guiding Principles. As a result, the FX Vision and Guiding Principles support the Agency's Mission, Vision, and Goals to effectively guide the Agency's investment decisions during the transition to a modular environment. The Agency's FX Vision is to *Transform the Medicaid Enterprise to provide the greatest quality, the best experience, and the highest value in health care.*

- Goal #1 – Improve Data Quality
 - › Objective #1 – Create reusable business and technical services that provide consistent data validation, edits, and transformation of data based on a single source of policy truth
 - › Objective #2 – Enable the use of business and technical services throughout the Agency that create, access, and maintain data consistently in a single source of data truth (e.g., Operational Data Store for transactional data and the Reporting Data Store, Enterprise Data Warehouse, and Data Marts that derive from the Operational Data Store)
 - › Objective #3 – Create business and technical services that perform real-time processing and enable real-time data access
- Goal # 2 – Improve Recipient and Provider Experience
 - › Objective #1 – Enable processing consistency across system, program, and organization boundaries
 - › Objective #2 – Enable complete and consistent data collection for MES business processes
 - › Objective #3 – Enable no-wrong door processing to increase access and information timeliness and accuracy

- Goal #3 – Reduce MES Total Cost of Ownership (TCO)
 - › Objective #1 – Reduce duplication of custom code embedded in applications that perform the same business or technical processing
 - › Objective #2 – Simplify testing of established services
 - › Objective #3 – Enable service versioning to reduce change management complexity
- Goal #4 - Encourage Service Reuse
 - › Objective #1 – Establish a registry that allows potential service consumers to identify existing or planned services that can be reused
 - › Objective # 2 – Simplify the ability to identify, create, and reuse business and technical services
- Goal #5 – Develop, document, and implement the necessary processes to maintain and update the Technical Management Strategy, Technical Architecture documentation, FX Projects Repository, and Technical Standards

5.4 DESIGN GOALS

Following a set of well-defined application development design principles improves the quality, consistency, and overall cost effectiveness of the FX application environment. The FX application architecture design principles are based on widely used standards and concepts currently used in building a sophisticated system to enable future expansion. The primary FX application architecture design principles are:

Data Normalization – Because data duplication leads to errors, there is a strong incentive to establish Single Source of Truth (SSOT) entities to achieve the goal that each fact be a single non-decomposable unit, where these facts are independent of all other facts. When a data change occurs, the expectation is only one data location requires modification.

Factoring – This principle is similar to Data Normalization but refers to application code. Well-planned architectures segment specific code functions or behaviors. At runtime, these appear as separate groups or layers, where each of these layers represent a level of abstraction or domain.

Automatic Propagation – Entails the need to maintain accuracy and consistency through disseminating changes in data or code across a disparate environment. This means that when it is necessary for performance sake to duplicate data or application code to maintain consistency and correctness, the update of these facts is automatic at construction time.

Minimize Functionality – If an application component exists that meets requirements, reuse that component or service wherever possible. Doing so provides the benefits of needing less code to write, verify, and maintain. It can also reduce memory and runtime resources. To support widespread reuse, an Application Service Registry (ASR) will track the inventory of reusable components and services. The ASR will support search and registration activities. Managing change to reusable components and supporting concurrent use of versions services reduces the operational complexity of change to services and reusable components. Designers and developers use the ASR to conduct impact analysis across all development and production environments. Identifying both direct impacts and secondary impacts all the way to the Business Service level simplifies management of shared components reducing the coordination effort. Likewise, the ASR can help track the use of previous service and component versions to reduce the overall maintenance efforts.

Construct Layers – To construct an extensible system, the construction process involves using intermediate layers, which can act on the data received from higher layers of the application architecture. These intermediate layers act like virtual machine engines that handle the processing of a specific function in a separate session. This allows data to define the specific functionality, which enables the layered components to be very reusable.

SECTION 6 PROPOSED SYSTEM

The proposed technical solution is to procure modules to replace business processes within the MMIS that are interoperable with other systems within the FX transformation program, using open source solutions, COTS products, or other modular approaches that reduce the need for custom development. Proposed solutions include IS/IP and EDW, and modular procurements for Provider Management, Centralized Contact Center, Core Processing (including Financial Management, Encounter Processing, and Claims Processing), Recipient Management / Enrollment Broker, Pharmacy Benefits Management, Plan Management, Third Party Liability, Enterprise Case Management, and Contractor Management.

The SEAS Vendor produced technical deliverables that defined the data management, technology, system design and implementation, and enterprise security management strategy for the program. Links to the various technical deliverables can be found in Appendix B.

6.1 TECHNICAL SOLUTION ALTERNATIVES

The evolution to modular applications decouples applications from proprietary data stores, leverages and provides reusable business and technical services, and uses enterprise integration platform services including security and business rule services.

To date the Agency had prepared to pursue a *Project-based modular* technology solution alternative that modernizes the Agency applications using a project-based evolution. Projects identified with each business area would facilitate the reorganization of existing systems into modular applications. Under this approach business outcome-based prioritization of projects chosen and sequenced from a portfolio of potential projects resulted in a dynamic implementation roadmap.

The Agency interviewed representatives from 11 other states and evaluated the applicability of the current strategy considering themes of other state technical transformations.

Figure 12: Other State Transformation Themes lists primary strategies states reported pursuing to modernize their Medicaid program delivery capability:

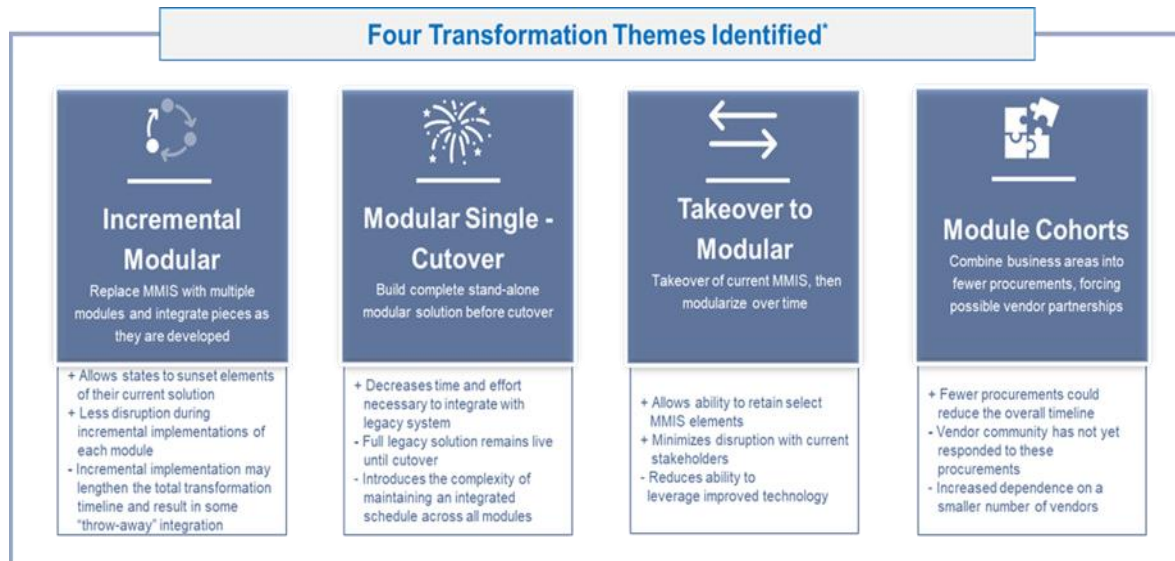


Figure 12: Other State Transformation Themes

- **Incremental Modular** - Replace MMIS with multiple modules and integrate pieces as they are developed – This alternative selects system(s) and operational processing performed for each business area and integrates the replacement module (systems and operational processing) through implementations or cut-overs for each business area. With this approach, vendors will replace the legacy components of the existing system with new modules until vendors modernize all components of all business areas.
- **Modular Single - Cutover** - Build complete stand-alone modular solution before cutover – This alternative selects, develops, integrates, and tests modular components and operational processing for all business areas and replaces the current processing through a single implementation or cut-over to the new systems that are made from modular components.
- **Takeover to Modular** - Takeover of current MMIS, then modularize over time – This alternative has a vendor takeover operation of the existing Fiscal Agent systems and operational processing responsibilities and requires the takeover vendor to replace current processing with modular solution components over time after completion of the takeover.
- **Module Cohorts** - Combine business areas into fewer procurements, forcing possible vendor partnerships – This alternative is a variation of the modular implementation that attempts to gain synergies by procuring and implementing a modular solution for business areas with significant interdependencies or synergies.

Error! Reference source not found. shows the pros and cons of each technical implementation approach alternative:

APPROACH	PROS	CONS
Incremental Modular	<ul style="list-style-type: none"> Allows states to sunset elements of their current solution Less disruption during incremental implementations of each module 	<ul style="list-style-type: none"> Incremental implementation may lengthen the total transformation timeline and result in some <i>throw-away</i> integration
Takeover to Modular	<ul style="list-style-type: none"> Allows the ability to retain select MMIS elements Minimizes disruption with current stakeholders 	<ul style="list-style-type: none"> Reduces the ability to leverage improved technology
Modular Single - Cutover	<ul style="list-style-type: none"> Decreases time and effort necessary to integrate with legacy system 	<ul style="list-style-type: none"> Full legacy solution remains live until cutover Introduces the complexity of maintaining an integrated schedule across all modules
Modular Cohorts	<ul style="list-style-type: none"> Fewer procurements could reduce the overall timeline 	<ul style="list-style-type: none"> Vendor community has not yet responded to these procurements Increased dependence on a smaller number of vendors
Project-based Modular	<ul style="list-style-type: none"> Faster realization of benefits and operational improvement Smaller more manageable projects 	<ul style="list-style-type: none"> Uncertainty about the timing of completing the transition of all current Fiscal Agent operations More projects to manage

Table 2: FX Implementation Approach Alternatives

6.2 RATIONALE FOR SELECTION

The recommended technical solution is to use an incremental modular evolution and consolidation strategy. The rationale for this approach includes:

- **Focus on transition of current operations performed by the current Fiscal Agent** to different vendors by 2024 to align with a legislative mandate and revised Agency Strategic Priorities
- **Improve the effectiveness of spending on the Fiscal Agent that accounts for ~ .05%** of the Agency’s annual budget spend by prioritizing Fiscal Agent related work into an initial phase
- **Reduce peak agency staffing requirements** by extending the overall FX Roadmap schedule and deferring transformational improvements that benefit stakeholders external to the Agency
- **Reduce FX program management complexity** by reducing the number of projects and interim production implementations
- **Reduce risk to current Fiscal Agent operations** and their ability to retain staff during the transition by reducing change, disruptions, and production processing changes
- **Reduce risk to current production operations** by reducing and delaying interim changes to production operations

- **Increase consistency of stakeholder communication** and visibility to stakeholder experience information about health plan, provider, and recipient interactions with the Agency by using a single Centralize Contact Center vendor
- **Simplify communications** and increase the understanding of the FX approach and schedule

Each modular application implementation is to align with the FX technology, information management, and security strategies and standards. The rationale for the technical solution is that:

- Technology modernization investments are driven by value generated and direct impact on supporting the business
- The chosen solution best supports key recommendations of data management and technology strategies in that it:
 - › Operates from a single source of truth for data
 - › Operates from a single source of truth for policy and business rules (e.g., data edits, validations, transformations, decision-making)
- Performs data validations at the point of the business event to improve data quality
- Aligns with expected market evolution in data management (e.g., toward Blockchain-like distributed ubiquitous data management)
- Enables a higher level of business agility and reduces costs to convert proprietary vendor data
- Reduces vendor lock-in and problems with vendors controlling access to Agency data

6.3 RECOMMENDED TECHNICAL SOLUTION

The FX Data Management Vision emphasizes six primary strategies that align with the overall FX strategic priorities and the recommended technical solution will be required to align with all six:

- Improve data quality by operating from a single source of policy truth
- Evolve core processing with data validation at the point of business event data collection
- Provide seamless access to a real-time, 360-degree view of recipient and provider information
- Decouple data from proprietary systems and application stores
- Operate with business area and persona optimized data marts and data analysis tools
- Prepare to collect and manage recipient and provider experience and outcome data

Improve data quality by operating from a single source of policy truth. Today, data edits, data validations, and data transformations are the electronic implementation of policy. The inconsistent application of data edits, validations, and transformations to the many different Agency data stores means there is no single source of policy truth which causes confusion and lack of trust in the data both within the Agency and with external consumers of Agency data. For example, data edit rules and policies are applied differently on the front-end of MMIS interChange when compared to the back-end processing resulting in claims rejections. Different business units and individuals

implement policy by applying specific data edits, validations, and transformations to their own data sets to meet their needs or preferences. Often, separate systems support different versions of data validation and transformation. When each business area can claim common data is not right for the unit, this leads to many propagations of duplicated data and no true single source of the truth. The Agency's strategy is to centralize and standardize data edits, data validations, and data transformations applying the policy to a single source of truth data set. After consolidation, a single set of policies operationalized as system edits, validations, and transformations decreases the need for business unit or individual specific clones of data. After a single source of policy truth exists, health plans and providers can use the electronic implementation of this policy to validate information before submission to Agency systems, reducing errors and rejects.

Evolve core processing with data validation at the point of business event data collection.

Today, high-volume claims and encounter processing occurs in a single system that validates submissions in a complex, difficult to maintain claims processing engine. The current system is a stable, reliable workhorse that is essential for timely and accurate payments to health providers in Florida. Naturally, there is reluctance to introduce risk to this critical processing engine because of the transaction volumes and State spending processed by the system. However, evolution of core claims and encounter processing is essential for the Agency to meet its mission and strategic priorities. The most significant improvements in provider experience, recipient experience, levels of fraud, and provider administrative costs depend on how core processing works. The Agency strategy is to evolve core processing by allowing health plans and providers to validate and verify claim and encounter data before submission to the Agency. Evolutions in core processing will reduce errors, rejected transactions, denied claims and encounters, and costs.

The Agency strategy to evolve core processing involves:

- Providing access to an electronic set of policy truth (e.g., implemented via rules engine)
- Providing health plans and providers with recipient, provider, and reference data needed for evaluation against the electronic set of policy truth
- Having health plans and providers validate and resolve errors before claim and encounter submission by validating data at the point of business event. This will be accomplished through services the Agency will expose to health plans and providers allowing them to validate data against edit rules and policies before submitting to the Agency
- Submitting validated claims and encounter records that can be accepted with minimal Agency processing

The Agency strategy of going beyond the boundaries of the Agency to fix data quality problems is foundational to address symptomatic and derivative issues that affect many business functions.

Provide seamless access to a real-time, 360° view of recipient information. Today, batch files drive most of Medicaid system processing. The Agency strategy is to use technology to assemble information in near real-time from all relevant sources to make processing decisions. The near real-time, 360° view of recipient information will eventually include information from other Medicaid stakeholder organizations providing access to comprehensive social determinants of care data. Access to current and complete recipient information will improve service authorization decisions, treatment, and enhance coordination of care by health plans and providers. The information will also help organizations in the community of care to deliver non-Medicaid services

to recipients. Providers of education, child welfare, elder care, employment, and other services can be more effective by leveraging information and collaborating with other providers to benefit the recipient. For example, another state's analysis of behavioral issues in schools leading to class disruption, detention, suspension, and expensive behavioral services found the root cause often originates from health issues related to vision, hearing, and dental screenings. By sharing claim or encounter information with appropriate data privacy protections, educators may accommodate children, provide proper referrals, and confirm that appropriate screenings occur. Providing service providers with real-time access to a comprehensive view of recipient information should also help the Agency, health plans, and providers to identify if increased coordination of care is prudent and justified.

Decouple data from proprietary systems and application stores. Today, MMIS and most application systems use tightly coupled databases that contain information structured for use in an individual application. The Agency data management strategy is to manage data as a service. New FX modular components operate using data access services that connect to an operational data store that is independent of specific systems or modules. The operational data store provides data to applications through service calls or APIs by subject areas, which is a commonly used and supported technical pattern. Decoupling data from proprietary systems and databases helps operate from a single source of the truth and reduces data duplication. This strategy simplifies access, improves security, and enables business agility to replace or improve a new module. Decoupling will also simplify the future migration to emerging virtual data access technologies (e.g., Blockchain) that allow entire industry ecosystems to contribute data, access data, and operate from a single secure information source.

Operate with business area and persona type optimized data marts and data analysis tools. As it relates to data strategy, a persona categorizes and defines the data and analytic usage and processing characteristics for a person. The persona generalizes the types and breadth of data used and processed and the types of tools used to perform a role. In most organizations, there are 5-10 different personas. Currently, several hundred Agency personnel routinely develop and execute custom Structured Query Language (SQL) queries in roles as power users. The Agency's data strategy is to provide optimized data marts and tools that meet the needs of each combination of business area and data processing persona type. For example, users that perform advanced data scientist level analytics may need access to pull the data into more sophisticated software programs such as SAS to analyze the data more effectively. A data mart to support some personas would allow for a large download in a quick and efficient manner directly by the users themselves. This new strategy should reduce costs and improve responsiveness to business needs by rightsizing technology spend based on business persona need.

Prepare to collect and manage recipient and provider experience and outcome data. Today, the Agency and the entire healthcare industry has limited visibility to comprehensive recipient and provider experience or health outcome data. Survey and sampling provide limited feedback mainly about recipient satisfaction with provider interactions. Across all industries, system and process improvements are raising expectations of recipients and providers. The Agency expects increased scrutiny on the overall costs, time spent, and quality of service interaction by recipients and providers in the delivery of healthcare services. For the Agency, health plans, and providers this

means collecting, storing, and analyzing more data and new types of data with new dimensions of analysis. Collecting experience data efficiently also requires new applications and technology. Likewise, emerging advanced payment models (e.g., Diagnosis Related Grouping (DRG), Enhanced Ambulatory Patient Grouping (EAPG), bundled payments) introduce changes to core claims and encounter processing systems.

6.4 PROPOSED SOLUTION DESCRIPTION

The proposed solution is to procure the services of the SEAS Vendor to develop the strategic plan for the FX transformation program and identify solutions that meet the current and future business needs of the Medicaid Enterprise. An IS/IP vendor will be procured to provide the technical expertise to perform systems integration and ensure the integrity and interoperability of systems within the Medicaid Enterprise. Additionally, the IS/IP vendor will integrate services and infrastructure within the Medicaid Enterprise without relying on a common platform or technology. The procurement of an Enterprise Data Warehouse will provide data warehousing and data integration capabilities that will provide a unified data repository for reporting and analytics. Modules will be procured to replace business processes within the MMIS that are interoperable with other systems within the Enterprise.

6.5 CONTEXT DIAGRAM

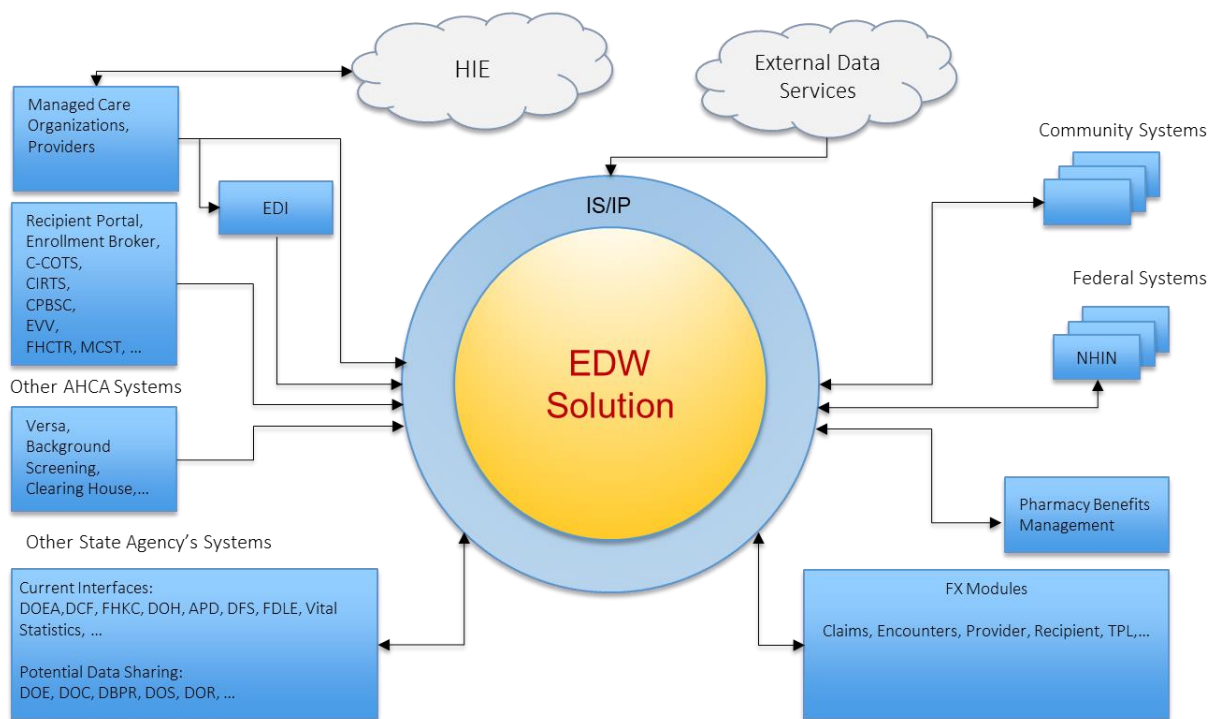


Figure 13: Context Diagram

6.6 HIGH-LEVEL OPERATIONAL REQUIREMENTS AND CHARACTERISTICS

6.6.1 USER COMMUNITY DESCRIPTION

- Recipients (including potential Recipients) – AHCA administers health coverage for vulnerable and underserved populations who might otherwise go without medical care for themselves and their children.
- Providers – The State is responsible for enabling access to covered services through a network of providers for which the State verifies credentials and licenses, including individual providers (i.e., doctors, nurses, social workers, dentists, and other ancillary providers) and facilities (i.e., hospitals, ambulatory surgery centers, assisted living facilities, nursing homes, and home health agencies).
- Federal and State Agency Partners – The State partners with independent partner agencies for information and data exchange related to providing care, including the CMS, Social Security Administration, Florida Department of Children and Families, Florida Department of Health, Florida Department of Elder Affairs, Florida Agency for Persons with Disabilities, and Office of the Attorney General Medicaid Control Fraud Unit (MFCU-OAG).
- Health Plans – The State carries out its mission through two models: Fee-For-Service (FFS), which directly manages care for members, and managed care through Statewide Medicaid Managed Care (SMMC), which manages an assigned group of members. Health plans are also responsible for credentialing their providers, managing the care delivered to members, and maintaining a network to provide adequate access to their covered members.
- Vendors – Many MMIS processes are contracted to outside vendors with contractual authority to perform various functions and interact with the core MMIS to send and retrieve current data.

User Group	Description / Expected Use of System	Type (Federal Employee, Contractor)	Geographic Location	Network Profile (LAN, WAN, External)	Total Users	Concurrent Users
Recipients	Access health benefits, verify coverage, change health plans or providers, track claims, communications	End User, Private Citizen	Statewide	External	Potentially over 3.8 million	Unknown
Providers	Verify coverage for recipients, submit and track claims, enroll as a Medicaid provider or a licensed/credentialed facility, correspondence	End User, usually a medical care provider or facility, or pharmacy	Statewide	External	Just under 150,000	Unknown
Centers for Medicare and Medicaid Services (CMS)	Exchange data on Medicare buy-in or disabled recipients	Federal		External		
Federally Facilitated Marketplace (FFM)	Verify Medicaid coverage for individuals applying for ACA coverage.	Federal		External		
Social Security Administration	Exchange data on Medicare buy-in or disabled recipients	Federal		External		
Department of Children and Families (DCF)	Determines eligibility for Medicaid recipients. Batch transmission of eligibility and enrollment files to the fiscal agent for plan assignment and coverage.	State Employee	Statewide	External		
Department of Health	Responsible for the regulation and licensing of health practitioners. Exchange data related to provider licensing.	State Employee	Statewide	External		
Department of Elder Affairs (DOEA)	Provides direct services through its Division of Statewide Community-Based Services and determines the level of care needed long term care recipients.	State Employee	Statewide	External		
Agency for Persons with Disabilities (APD)	Provides access to community-based services, treatment, and residential options for the developmentally disabled.	State Employee	Statewide	External		
Office of Attorney General Medicaid Fraud Control Unit (MFCU-OAG)	Investigates and prosecutes fraud involving providers that intentionally defraud the state's Medicaid program through fraudulent billing practices.	State Employee	Statewide	External		
Health Plans	Manage an assigned group of members. Health plans are also responsible for credentialing their providers, managing the care delivered to members, and maintaining a network to provide adequate access to their covered members.	Contractor	Statewide	External		
Vendors	A variety of vendors contract with the Agency to perform various functions (ex: pharmacy benefits, choice counseling, provider network verification, etc.) and interact with the MMIS to send and retrieve current data.	Contractor	Statewide	External		

Table 3: User Community Description

6.6.2 NON-FUNCTIONAL REQUIREMENTS

6.6.2.1 SECURITY AND PRIVACY CONSIDERATIONS

FMMIS maintains current and historical Protected Health Information (PHI) and Personally Identifiable Information (PII) for providers, recipients, and recipient households. Because this data may be shared with other entities within the state to support additional processing, it is vital the information is protected throughout the capture, processing, transmission, online usage, and storage of this data. Accordingly, all stakeholders accessing data within the new system in any manner will be required to go through proper security credential verification. The new system must comply with the following security and privacy standards:

NAME	DESCRIPTION	GOVERNING BODY	STATUTORY REFERENCE
Security Standards for the Protection of Electronic Protected Health Information	Commonly referred to as the HIPAA Security Rule . Provides specific standards and safeguards for health information protection	Federal Government	45 CFR Part 164, Subpart C
Federal Information Security Modernization Act of 2014	Establishes the Secretary of Homeland Security as the responsible party to implement policies and practices to secure Federal information systems	Federal Government (Department of Homeland Security)	S.2521 of the 113 th Congress to amend Chapter 35 of Title 44, United States Code
Federal Information Processing Standards	Sets the approved technical standards and guidelines for federal information systems	Federal Government (NIST)	S.1124 of the 104 th Congress – Information Technology Reform Act of 1996
Medicaid Information Technology Architecture (MITA) Framework	Provides authority for states to receive enhanced federal funding by developing highly interactive and interoperable MES platforms	Federal Government CMS	Affordable Care Act: Medicaid Program: Federal Funding for Medicaid Eligibility Determination and Enrollment Activities (CFR Vol. 76, No. 75)
Florida Cybersecurity Standards	Establishes the Florida Cybersecurity Standards (FCS), the minimum standards for state agencies to secure IT resources. Uses the NIST CSF and Federal Information Security Management Act (FISMA) as guiding documents	State of Florida	60GG-2.001 through 60GG-2.006, Florida Administrative Code

NAME	DESCRIPTION	GOVERNING BODY	STATUTORY REFERENCE
Florida Technology Architecture Standards – Identity Management	Creates the Identity Management Services framework to provide secure, reliable, and interoperable mechanisms for authenticating the identity of devices, application services, and users that consume state information and application resources. This rule is modeled after the Identity Ecosystem Framework Baseline Functional Requirements v1.0	State of Florida	60GG-5.003, Florida Administrative Code
SEAS Contract	Authorizes the Florida Agency for Health Care Administration to expend funds in support of developing the strategy and governance for the State’s MES transition	Florida Agency for Health Care Administration	SEAS Contract MED-191

Table 4: Security and Privacy Standards

By implementing a comprehensive and robust security scheme around the Medicaid Enterprise, the Agency avoids these risks:

- Unauthorized access to PHI and PII
- Monetary damages due to unauthorized access to PHI and PII
- Compromising data integrity
- Stakeholder dissatisfaction

6.6.2.2 AVAILABILITY REQUIREMENTS

System availability requirements are outlined in the table below:

System Availability Requirements	
Solution Availability	Excluding Agency-approved downtime for maintenance, the Solution shall be available, at a minimum, 99.982% of the time, twenty-four (24) hours per day, seven (7) days per week.
Approved Downtime	All Planned downtime and maintenance outages shall be coordinated with and approved by the Agency at least five (5) business days in advance and must occur after 10:00 PM ET and

	before 6:00 AM ET, unless a different time is approved by the Agency.
Notification	Agency staff shall be notified by email twelve (12) hours before any scheduled maintenance.
Recovery Time Objective (RTO) and Recovery Point Objective (RPO)	In the event of unscheduled system outage, the RTO shall be no more than 2 hours and RPO shall be no more than 15 minutes.

Table 5: System Availability Requirements

6.6.2.3 VOLUME AND PERFORMANCE EXPECTATIONS

The following capacity, performance, and availability expectations have influenced the technical design of the FX. System volume and performance expectations are depicted in the following tables:

Current Volumetric Capacity	
Volumetric Type	Volumes
Number of Systems/Applications	149
Total Number of Internal Users	8,815
Total Number of External Users	352,754
Number of Concurrent Users	1,983
Number of Outbound Interfaces	139
Number of Inbound Interfaces	126
Number of Databases Types	199
OLTP Database Size (TB)	32
Avg Volume of Transactions Per Day	11,261,530
Number of Real Application Clusters (RAC) Nodes	21,005
Avg Backup Size (GB)	30,127
Avg Yearly Data Growth (TB)	9
Number of Published Reports	2,679
Content Management Database Size (TB)	55
DSS Database Size (TB)	16
Number of DataMarts	11

Table 6: Current Volumetric Capacity

Performance Expectations	
Response Time – IS/IP	The IS/IP solution shall process data received from real-time interfaces and be accessible to the system less than one (1) second at least 99.5% of the time
Enterprise Data Warehouse Data Currency	The solution shall maintain a level of data currency in the Enterprise Data Warehouse where committed source data is available based on intervals specified by the Agency; daily source data is available in the target system within 24 hours; Weekly, Monthly, Quarterly, Annual and Odd Cycle source data shall be available in the target system within 72 hours
Reporting Data Store Data Currency	The solution shall maintain a level of data currency in the Reporting Data Store where committed real time source data is available within 5 minutes, committed delayed source data is available in the target system within 60 minutes, committed daily source data is available in the target system within 24 hours; Weekly, Monthly, Quarterly, Annual and Odd Cycle source data shall be available in the target system within 72 hours
Response Time - Data Service Request	The solution shall be capable of responding to simple data service requests in less than 125 ms (milliseconds), data service requests of medium complexity in less than 140 ms, and complex data service requests in less than 170 ms
Response Time – Direct Access	The solution shall be capable of responding to simple direct access queries in less than 25 ms, direct access queries of medium complexity in less than 40 ms, and complex direct access queries in less than 70 ms
Response Time – Reports	The solution has response times to simple reports within 1 second, reports of medium complexity within 2 seconds, and complex reports within 3 seconds
Response Time – Provider	The Provider solution shall support and maintain the Data Management, Data Security, and Data Quality of all data received by the solution and that maintains data integrity throughout all Replication and ETL (Extract-Transform-Load) processes

Table 7: Performance Expectations

6.7 HIGH LEVEL ARCHITECTURE & ALTERNATIVES ANALYSIS

Error! Reference source not found. lists the primary High-level Architecture components and strategic direction of the FX modular implementation.

Alternative	Description	Pros	Cons	Rationale
Enterprise Integration Platform (IS/IP)	Provides enterprise service bus / API gateway, single sign-on, secure file transmission management used for integration of services, and APIs by modules and external systems	<p>Reduces integration effort for modules</p> <p>Enables secure information sharing and reuse</p> <p>Reduces ongoing integration Operations and Maintenance (O&M)</p>	Requires initial coordination between the IS/IP vendor and system interface partners	<ul style="list-style-type: none"> The Integration Services and Integration Platform is a foundational component to be used for integration between modules and external systems and services
Enterprise Master Data Management (IS/IP)	Provides identity matching services and a single source of truth for master person and master organization indexes that promote integration, reuse, and coordination of care	<p>Provides understanding of common recipients or providers across organizations and systems</p> <p>Identifies duplicate master records</p>	Requires some data governance and cross organization coordination	<ul style="list-style-type: none"> The Enterprise Master Data Management architecture is a foundational component that is essential to provide a 360-degree view of information and publish subscribe alerting that enables coordination of care

<p>Enterprise Business Rules Management (IS/IP)</p>	<p>Provides an enterprise business rules engine, business rules repository, and business rules interoperability for modules to execute rules-based decision services</p>	<p>Enables policy and business rules interoperability and consistency between stakeholders</p> <p>Enables reusable business rules services</p> <p>Provides transparency to policy and basis for decision</p>	<p>Modules with proprietary rules engines may object to standards and coordination</p>	<ul style="list-style-type: none"> The Enterprise Business Rules Management solution improves the maintainability and consistency of business rules use in different systems. Provides solution to meet CMS modularity standards and conditions
<p>Application Lifecycle Management (IS/IP)</p>	<p>Enterprise system development repository and processes to manage requirements and system development artifacts through analysis, design, development, testing, and ongoing operations phases</p>	<p>Improves solution quality and reduces development cost</p> <p>Enables perform cross module impact analysis</p>	<p>Vendors need to work collaboratively</p> <p>Some tool administration</p>	<ul style="list-style-type: none"> As opposed to every vendor having their own methodology and control of requirements the ALM supports management traceability and impact analysis; the ALM solution allows cross module life cycle management
<p>Enterprise Operational Data Store</p>	<p>Enterprise data services and data store that provides abstractions of data from applications</p>	<p>Improves data consistency and reuse</p> <p>Reduces vendor dependence</p> <p>Enables business</p>	<p>Vendors with tightly coupled proprietary data solutions may resist</p> <p>Requires common definitions of data subject areas and</p>	<ul style="list-style-type: none"> Provides data access services that enables systems to operate based on abstracted subject areas as opposed to proprietary module data solutions

		area innovation	attributes	
Enterprise Data Warehouse	Enterprise reporting data store, data warehouse, and persona optimized data marts used for dashboards, reporting, and analysis	Improves data timeliness and data consistency Reduces data management costs	Vendors that want to control data access may resist	<ul style="list-style-type: none"> • Modernizes analytic data management, processing capacity, and provides capabilities optimized to support different types of data analysis
Enterprise Analytics and Reporting	Tools and operational responsibility to develop, maintain, and produce dashboards; reports from the enterprise data warehouse	Improves effectiveness of operational and analytic personnel	Some vendors may resist because they want to control data analytics	<ul style="list-style-type: none"> • Modernizes analytic and reporting tools. Simplifies analytic and reporting of data that crosses business areas
IT Common Operations	Provides enterprise managed services that can be reused by multiple modules	Provides standardization that improves operations and reduces costs	Use requires coordination Distributes vendor accountability	<ul style="list-style-type: none"> • Provides vendors guidance on the degree of standardization, acceptable solutions, and enables reusable enterprise solutions that enable standardization and synergies
Business Area Modular System	Business areas provide systems and operations and maintenance for systems. Generally, business area module solutions are not to provide or manage proprietary business area data solutions or business processing operations	Improves Agency business agility Increases vendor market competition	Module vendor economics are changed without contact center or business operations scope Module vendor may resist not controlling data or because their solutions can be	<ul style="list-style-type: none"> • Module approach that focuses on achieving benefits, reducing maintenance and operations, increasing access to business area innovation, and reducing future module transition and conversion costs

			displaced easily	
Centralized Contact Center Platform	Common unified contact management infrastructure to manage inbound and outbound interactions with stakeholders through a wide variety of channels	Improves the ability to understand and analyze stakeholder experience and interaction data Provide more consistent interaction experience	Some vendors may have contact centers optimized for the business area of their system	<ul style="list-style-type: none"> Increases collection, access, and analysis of stakeholder interaction data. Reduces duplication and inconsistency of vendor contact management solutions
Enterprise Case Management Platform	A low code enterprise solution used to manage a wide range of cases that involve defined and undefined processes, workflow, and case management services	Easy to implement and maintain case management processes	Platform may offer duplicate capabilities to FX enterprise capabilities requiring integration	<ul style="list-style-type: none"> Simplifies and standardizes the creation of case management processes used to manage a wide variety of case types
Centralized Contact Center Operations	A designated vendor that provides personnel (e.g., contact center agents) that respond to stakeholder interactions	Provides consistent stakeholder contact experience Provides contact center capacity, scale, and contingency not available with some module vendors	Vendors interested in contact center operations may resist Certain types of contacts require specialized skills Changes module vendor	<ul style="list-style-type: none"> Consolidates stakeholder experience accountability across business areas or historic contract responsibilities

			accountability expectations	
Centralized Business Operations	A designated vendor that provides personnel that perform business operations (e.g., processing enrollment applications, resolving claim issues)	Provides accountability across business areas Provides business processing capacity, scale, and contingency not available with some module vendors	Vendors interested in business operations may resist	<ul style="list-style-type: none"> Consolidates accountability across business areas or historic contract

Table 8: Solution Design Alternatives

6.7.1 APPLICATION ARCHITECTURE

The Application Architecture connects Business Services with Technical Services, as shown in **Figure 14: Conceptual Technical Architecture Diagram**. The Agency tailors Business Services to environmental needs. The Application Architecture framework defines services from the abstract level to the design level, which allows the Agency to build service interfaces as standard interfaces without dialects caused by interpretations.

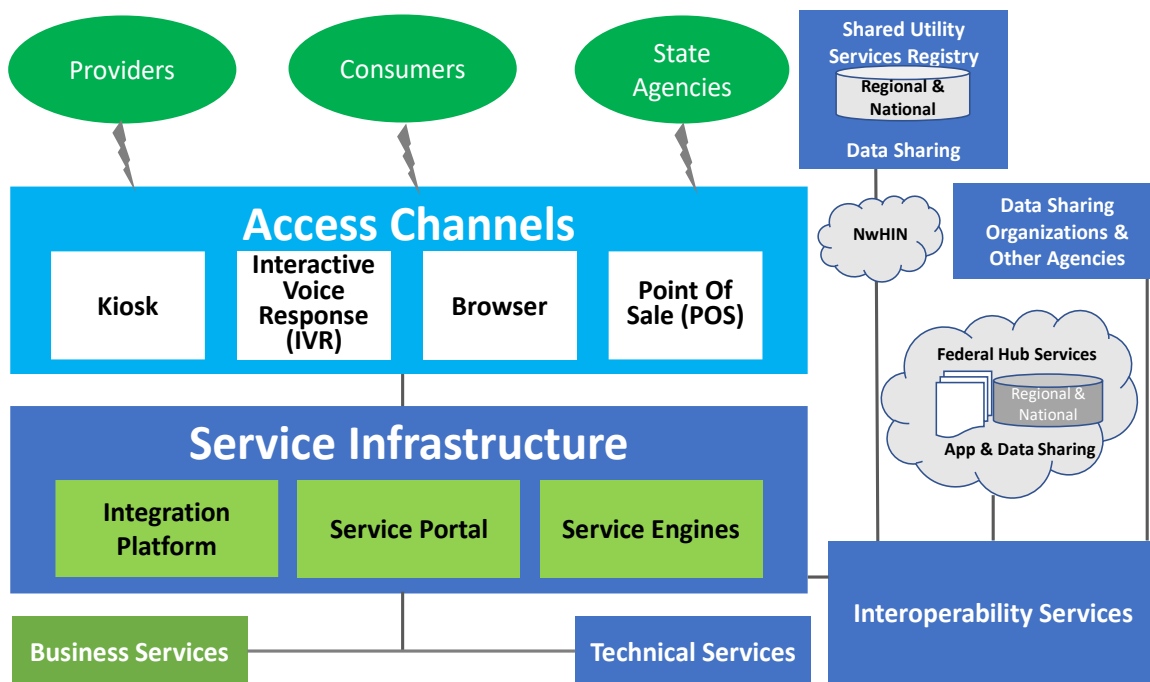


Figure 14: Conceptual Technical Architecture Diagram

The service infrastructure includes standards-based elements that use service-process integration and data sharing with other organizations and agencies. The Application Architecture framework is compatible with the Federal Health Architecture (FHA), the Nationwide Health Information Network (NwHIN), regional and national shared data sources, and the network on Regional Health Information Organizations (RHIOs). The Application Architecture framework defines a series of interoperability services based on Web Services (WS) and Extensible Markup Language (XML) message formats and protocols. The tools the Agency requires to establish interoperability, data capabilities, and other support requirements, are available to the Agency in groups using common facilities.

The following sections provide a description of the top-level Application Architecture Service Oriented Architecture (SOA). They describe fundamental infrastructure components, such as the Enterprise Service Bus (ESB), the Service Management Engine (SME), infrastructure services (e.g., external data-sharing and hubs), and provide references to industry standards.

A multilayer Application Architecture model represents a combination of applications and connections to deliver services to stakeholders, as shown in **Figure 15: Multilayer Application**

Architecture Model. The four (4) levels are the Access Layer, Service Management Layer, Service Application Layer, and Platform Layer.

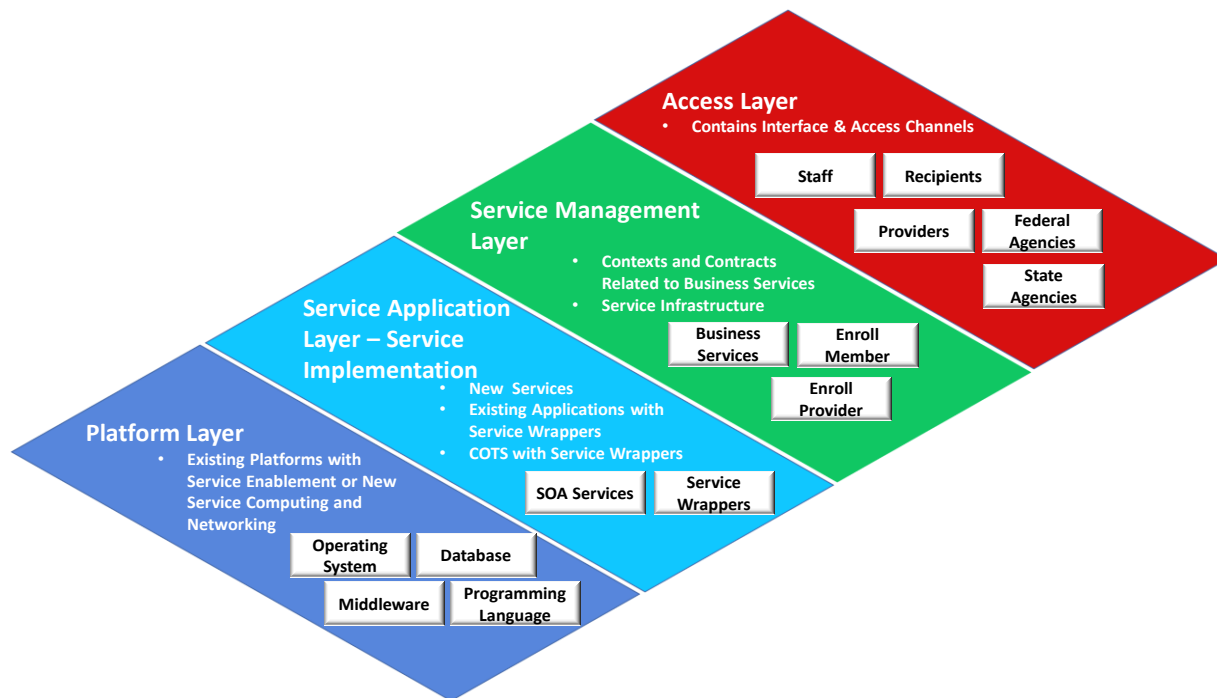


Figure 15: Multilayer Application Architecture Model

- **Access Layer** – This layer is where end users connect to the application. This is most likely through a user interface like a web page. Additionally, this could be via a web service or API accessed by an internal or external system.
- **Service Management Layer** – This layer consists of the service infrastructure, service contexts, and service contracts for each Business Service. All Business and Technical Services are exposed via this layer. The Service Management Layer links to the Service Application Layer, either directly or through service wrappers.
- **Service Application Layer** – This layer consists of Data and Business rules services. Although the Service Application Layer consists of services, those services might be new services, wrapped legacy applications, or wrapped-COTS products. The Service Application Layer evolves incrementally as new applications are added.
- **Platform Layer** – This layer includes the software that is necessary to support the execution of the Application Layer.

6.7.2 INFORMATION ARCHITECTURE

A Conceptual Data Model (CDM) helps in identifying high-level key business and system entities and establishing the relationships existing between them. It also helps in defining the key issues of business problems and opportunities for the system. It can address both digital and non-digital

concepts. A conceptual data model can also help in closing the gaps between a solution model and requirements document.

The CDM has two levels, an Enterprise Conceptual Data Model (ECDM), containing all required data elements, and a MITA business process-specific set of CDMs for each business area. These are delivered as high-level data models, normalized to show *data classes* and *relationships* (associations between classes).

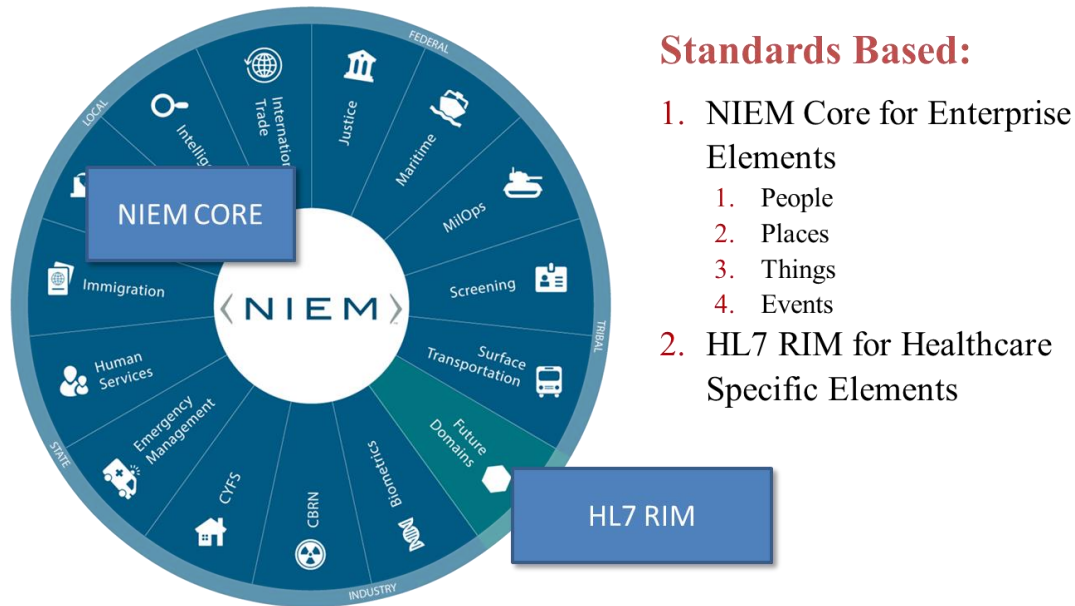
The FX data dimensions shows a general overview of the kinds of data each business area contains. This section of the deliverable will continue to develop and serve as the documentation for information architecture elements as they are conceived through the implementation of future module procurements.

The FX conceptual data models will follow and use applicable standards provided by national standards organizations, and State and CMS guidelines. The FX CDM will use applicable data classes and predefined names preferred by national naming standards:

- National Information Exchange Model (NIEM) version 4, for *core data* class names such as ORGANIZATION and PERSON, ENTITY as the superclass for any business party, ACTIVITY to represent a business event, IDENTITY, LOCATION, and ADDRESS
- Applicable data naming and data elements from other NIEM datasets
- Applicable data naming and data elements from Health Level 7 (HL7) Reference Information Model (RIM) datasets
- Applicable HL7 Fast Healthcare Interoperability Resources (FHIR) which are definitions aligned with the HL7 RIM
- NIEM version 4, for non-healthcare (e.g., non- FHIR) related class names

Figure 16:National Information Exchange Model version 4 provides the basis for modeling information exchanged especially between government organizations. NIEM is a canonical model that is the standard for exchange of information between government information sources. The federal government mandates use of NIEM for exchange of information between federal government organizations. NIEM is also widely adopted for modeling and exchange of information between other government data.

The use of NIEM based modeling and data vocabulary is a change from existing healthcare vocabulary that will require communication and organizational change management to secure adoption. The direction to use NIEM supports the direction for MITA higher maturity levels to increase integration and use of information across program, agency, and state boundaries. Likewise, the direction to use social determinants of care to increase coordination of health care will integrate new information sources and data types, and expand and change the vocabulary and perspective of the business. This evolution in vocabulary should be minor but will help particularly in communication with external organizations that already communicate with this vocabulary.



Standards Based:

1. NIEM Core for Enterprise Elements
 1. People
 2. Places
 3. Things
 4. Events
2. HL7 RIM for Healthcare Specific Elements

Figure 16: National Information Exchange Model

NIEM lacks data classes or elements defined for some of the healthcare specific data classes necessary for the Agency’s data model. Other federal agencies are transforming their models to NIEM. For these and other areas not supported by NIEM conventions, the data naming and formats will use standards from HL7 and the Federal Health Information Model (FHIM). FHIM is a national program supported by the federal government that provides a community of users, tools, common terminology, governance, methodologies, and support that enables enterprise-wide information exchange.

FHIR (pronounced fire) is the CMS specified health care information exchange standard describing data formats and elements (known as resources) and an API for exchanging electronic health records. The HL7 FHIR standard defines how healthcare information can be exchanged between different computer systems regardless of how it is stored in those systems. It allows healthcare information, including clinical and administrative data, to be available securely to those who have a need to access it, and to those who have the right to do so for the benefit of a patient receiving care. The standards development organization HL7 uses a collaborative approach to develop and upgrade FHIR.

Figure 17: Conceptual Data Model Sample represents the current CDM for the MMIS.

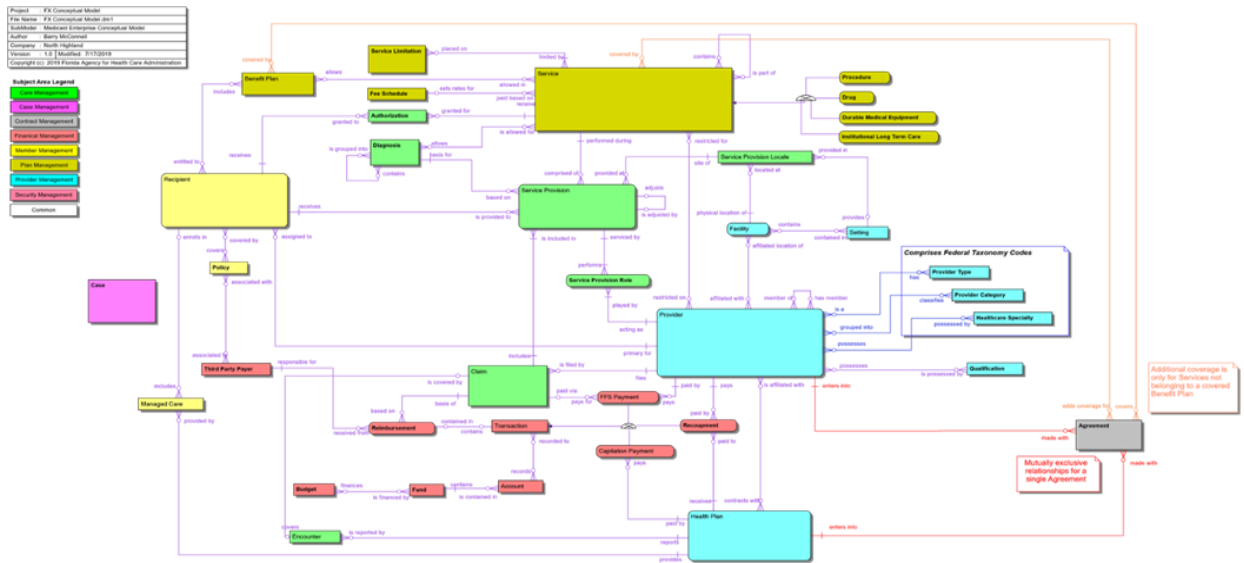


Figure 17: Conceptual Data Model Sample

The strategy to develop the FX CDM is to iteratively model the conceptual data and relationships relevant to FX Project implementations. This approach begins with a blank model and incrementally adds conceptual data model subjects for areas relevant to active FX projects. This deliverable creates an initial FX CDM by projecting the data types used in FX projects in the FX Infrastructure Phase of the FX procurement strategy. Specifically, this deliverable contains representative conceptual data modeling to support the anticipated processing of the IS/IP Project. This iteration models the conceptual data relationships used in integration and information exchange processing:

- Entity - people and organizations used in Master Person Index, Master Organization Index, and Master Data Management identity processing
- Integration Management – integration message information used in Enterprise Service Bus processing
- Security Management – system user identity credentials, authentication, and access control information used in single sign-on processing

Following the selection of a specific IS/IP vendor and solution, the SEAS Vendor will update the FX CDM for these areas to reflect additional data types and relationships managed by the integration solution. As the FX Project defines, procures, and implements other FX projects, the SEAS Vendor will elaborate the FX CDM until the FX CDM reflects all data subjects and relationships.

6.7.3 INTERFACE ARCHITECTURE

The Agency’s preference for increased granularity of enterprise functionality and an API-centered approach to seamless interoperability places particular design and delivery considerations on the underlying technical and interface architectures and foundational technologies of the FX. This is especially true of technical design considerations targeting and enabling the desired business process improvements essential to achieving the Agency’s goals. Many of these anticipated improvements are to be made possible by the functional and technical innovations amplified by proven, advanced system integration techniques and technologies.

The Agency fully understands the necessity to transition to a more up-to-date and advanced form of system integration in response to growing healthcare industry recognition that many stakeholder experience and business process improvement benefits are tied to creating a distinct data layer. Benefits are derived from improving upon and scaling intra-enterprise information data interchange messaging and inter-agency and trading partner information exchange.

The State is being intentional in risk mitigation actions and technical and information architecture capabilities to be implemented to avoid the risks of modularity damaging data integrity, data quality, and stakeholder interaction experiences. This risk avoidance is particularly focused on the early stages of FX implementation actions when the portfolio of functionality contains both new and legacy systems and modules.

The future MMIS will use new APIs and reuse existing APIs where possible and appropriate. All APIs will strictly follow Agency guidelines, governance, processes, and best practices. The development of individual APIs for each vendor and/or module will be designed following normative specifications. All API information will be maintained in an API inventory and registry.

Table 9: MMIS Interfaces presents key interfaces required to support MMIS processing and reporting.

INFORMATION SHARED	INTERFACING APPLICATION	PURPOSE	INBOUND OR OUTBOUND?	BATCH OR NEAR REAL TIME?	DATA STORED PERSISTENTLY?
MMIS Transactional Data from Vendors	MMIS Vendor Modules will use APIs	This is the data that is retrieved and/or sent from the Vendors’ systems modules. This data will end up in the ODS	Inbound/ Outbound	Batch / online real time	Yes
Federal and State Transactional Data	APIs designed for Federal and State Agencies	This is the data that is retrieved and/or sent from the State and Federal Agencies’	Inbound/ Outbound	Batch / online real time	Yes

INFORMATION SHARED	INTERFACING APPLICATION	PURPOSE	INBOUND OR OUTBOUND?	BATCH OR NEAR REAL TIME?	DATA STORED PERSISTENTLY?
		systems modules. This data will end up in the ODS			
MMIS Analytical Data	API designed for EDW interface	This is the data that is sent from MMIS. This data will end up in the EDW	Outbound	Batch / online real time	Yes

Table 9: MMIS Interfaces

6.7.4 TECHNOLOGY ARCHITECTURE

The technology architecture envisioned by the Agency and the SEAS Vendor will adhere to MITA principles, standards, and architecture configurations with a target of advancing MITA maturity levels. The following sections outline the future-state technology architecture as currently conceptualized, with several decisions still to be determined. The MMIS ConOps, along with the future-state system plan, shall be updated on an iterative basis as CMS provides new guidance, and as the Agency regularly assesses options and evaluates decisions.

6.7.4.1 PLATFORM

The Agency’s FX platform will be designed to provide a transition from the current application systems into loosely coupled, API-focused modules. This platform will consist of standardized APIs for core shared services, shared tools and resources, and an operational data store. The core shared services will provide critical functionality to multiple modules, and it will allow reuse of functionality by exposing services from other modules. The shared tools will expose access to tool functionality through the platform and will allow access to the tools from multiple modules. The operational data store will track transactional data and additional information for reporting and querying. The platform will focus on the use of technical standards, COTS, and open source tools. In addition, the platform will be developed using industry standards and deployed in virtualized servers on high end server architecture.

6.7.4.2 SYSTEM HOSTING

The Agency will require all vendors to develop and implement appropriate hosting environments capable of supporting all current and anticipated hosting and infrastructure needs. The MMIS ConOps will be updated concerning this topic on an iterative basis as the available options become more apparent, and a direction is solidified.

6.7.4.3 CONNECTIVITY REQUIREMENTS

The Agency will use its existing network infrastructure in conjunction with network infrastructure provided by the IS/IP and EDW vendors to address the anticipated connectivity requirements. The MMIS ConOps will be updated concerning this topic on an iterative basis as the available options become more apparent, and a direction is solidified.

6.7.4.4 MODES OF OPERATIONS

The IS/IP Vendor will be responsible for designing the hosting infrastructure along with the various environments necessary for development, testing, and operation of the Integration Platform. As illustrated in **Figure 18: Conceptual View of Multiple Environments**, supporting the integration platform will require a multi-environment strategy.

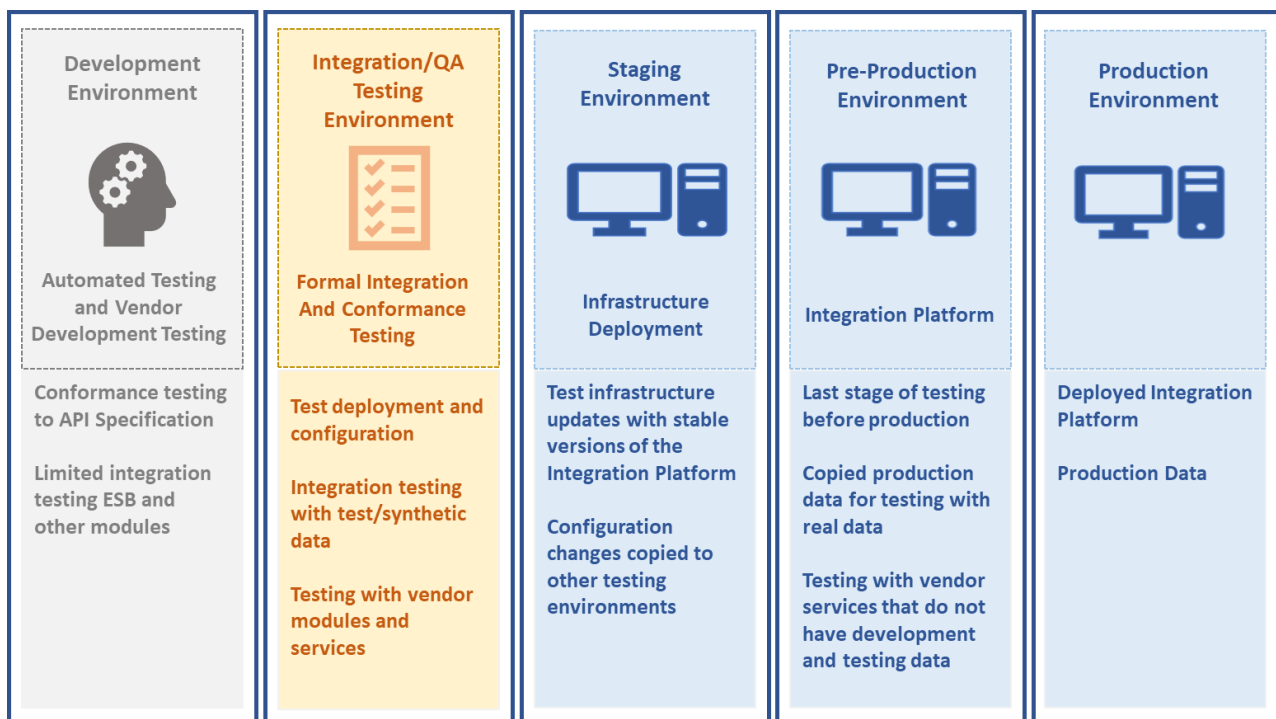


Figure 18: Conceptual View of Multiple Environments

The Development Environment runs the latest code and configuration from development through automated testing to identify deployment issues as early as possible. Deployment and configuration of the integration platform and APIs will be performed in the Integration/Quality Assurance (QA)/Test Environment. Vendor Development and Integration/QA/Test Environment connectivity is only possible with test data. Some vendors may only be able to test with production data and unable to participate in testing in these environments. Verification of infrastructure updates will be tested in the Staging Environment before the last stage of testing in the Pre-Production Environment with real data.

6.7.5 SECURITY AND PRIVACY ARCHITECTURE

An IS/IP solution will be implemented for FX, including both the technical means for authorized users to authenticate to the system and policies and procedures to support user vetting, credentialing, and identity life cycle management. Existing user roles and the system access available in the current solution will be used as a starting point for establishing roles, privileges, and permissions. The IS/IP will provide the authentication, authorization, and encryption components of the Integration Platform which encompasses the following capabilities:

- Single sign-on - The capability to authenticate once and be subsequently and automatically authenticated when accessing various target systems.
- Identity and access control - Enables the right individuals to access the right resources at the right times for the right reasons.
- Federated identity management - Enables identity information to be developed and shared among several entities and across trusted domains.
- Data anonymization - Tools and processes to sanitize information and protect privacy.

These security capabilities are to provide application or module level authentication. The goal is to provide role and content-based access control for information exchanged using the Integration Platform that will include controls at the page, action, and field level within applications or modules.

The solution will support external systems such as FX modular components which use custom access control strategies within each system or module and shall include enabling an encrypted bi-directional interface between the authentication service and the authorization service, allowing user information to flow between the two components. The authorization product shall provide federated integration with organization specific Active Directories of authorization information. Consent management is a possible future Integration Platform capability currently under consideration.

6.7.5.1 AUTHENTICATION

The IS/IP solution will authenticate all users accessing FX through a stakeholder single sign-on portal or system API interfaces. Security protocols and standards which follow the NIST 800-53 profile for *moderate impact systems* with additions and applicable state and agency standards and requirements are outlined in the MITA 3.0 security requirement document.

Vendors will require APIs to send or receive data from FX. Any vendor hosting their own solution will be required to submit and follow a security plan that adheres to the NIST 800-53 profile for *moderate impact systems* with additions and applicable state and agency standards and requirements.

6.7.5.2 AUTHORIZATION

The Agency will require any vendor to provide an authentication and the authorization scheme which follows the NIST 800-53 profile for *moderate impact systems* with additions and applicable state and agency standards and requirements for user access to authorized functions and systems.

6.7.5.3 ENCRYPTION

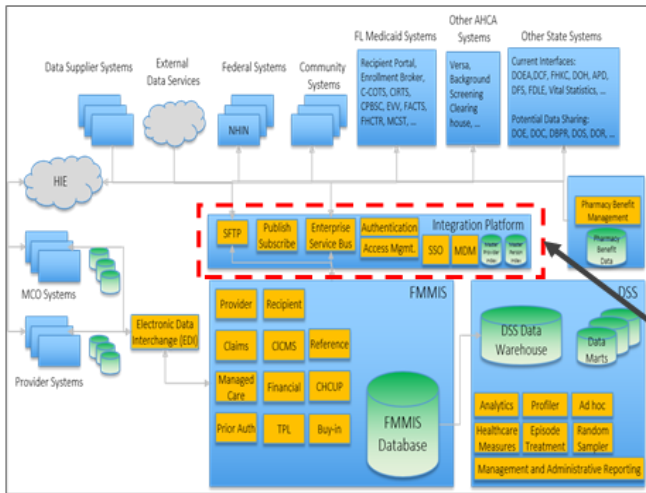
Due to the nature of the information and associated business risks, all PHI and PII will be encrypted for system receipt or handoff. Furthermore, all transmissions of data to the data warehouse will be encrypted. The following encryption standards will be implemented within MMIS regarding email, backup tapes, WEB interactions, and server interactions:

- Secure Socket Layers (SSL)
- AES-256 (Advanced Encryption Standard) encryption
- NIST approve transmission protocol
- WEB Certifications / bit key 256

The Agency requires vendors to obtain third party security assessment reports annually and submit them to the Agency for evaluation at which point the Agency will either recertify or require security system updates or changes according to a remediation plan.

Additional encryption requirements are as follows:

- **FIPS Encryption:** Federal Information Processing Standard (FIPS) 140-2 level 1 encryption used on HNC data connections between sites.
- **Data-at-Rest Encryption:** All Virtual Private Cloud and traditional Backup and Restore (BUR) storage compartments will be provisioned with *data at rest* encryption enabled.
- **Conversion/Development/Testing Data:** The database and application tiers for development, testing, and conversion will be separated to ensure that appropriate levels of access are granted. Development and testing areas that may be used by offshore developers and testers will be well-defined, compartmented, and use only de-identified data, using Agency-approved security protocols.
- **Data-In-motion Encryption:** Any inbound and outbound data transmissions must adhere to the FIPS Encryption noted above, this includes data across individual connections, used by Agency stakeholders.
- **Remote Access:** All Virtual Private Network (VPN) remote access methods to the network compartments use SSL encryption.



AHCA is procuring the IS/IP, which includes the Enterprise Service Bus, System Integrator, and Enterprise Information Management. The IS/IP will enable secure real-time, or near real-time information exchange between systems while migration to data services occurs. This allows for implementation of modular capabilities that interact with legacy systems and other modular capabilities.

This implementation will also enable integration of non-Medicaid data sources and system integrations with MMIS business processing. Integrations between MMIS modular capabilities and non-Medicaid data sources and information types will use the integration services indefinitely.

To allow for future data types and decisions, the Agency is designing the IS/IP to be as flexible and scalable as possible.

This state is categorized by the following:

- Real-time, or near real-time, data sharing and reuse through the IS/IP is routine
- Identify duplicate recipient and provider links, link identified records across systems through Master Person and Master Provider Indexes
- Single sign-on, authorization, and access controls to support sharing data and processing services across systems and modular processing
- Improved secure file transfer capabilities
- An ability to send select real-time transaction data to the data warehouse to support real-time analytics and reporting

Figure 19: FX Security Description

SECTION 7 ANALYSIS OF THE PROPOSED SYSTEM

7.1 IMPACT ANALYSIS

7.1.1 OPERATIONAL IMPACTS

The enterprise integration capabilities of the IS/IP solution will allow Agency systems to be much more efficient in sharing data and services between systems within AHCA and with other agencies. Two major goals of the integration platform are (1) reduced duplication of data across systems, and (2) improved data consistency and communication of data changes between systems when there is a business need for data to be duplicated.

The IS/IP, will enable:

- Near real-time data, processing, access, and sharing between different organizations and systems, reducing the propagation of duplicated and inconsistent data
- A 360-degree view of information by linking data about recipients and providers
- Application of consistent business rules and policy
- Single sign-on and data protections

The enterprise data service and analytic capabilities of the EDW solution will provide Agency stakeholders with enhanced data management and analytics capabilities. The EDW creates a model that promotes having a *single source of truth* for applications to provide and access data from this central source (rather than keeping data within each application). The EDW Project decouples systems and data to make data available and consistent throughout the ecosystem, which will improve data quality, consistency, and tools for operational data use and analytic processing. The EDW solution will enable:

- A single source of truth to improve data quality, accuracy, and accessibility
- Improved timeliness and consistency of data
- Improved analytic data processing with holistic business unit and persona optimized data marts and tools
- System innovation and simplified system implementation
- The ability to eliminate inconsistent data and processing
- Reduction in duplicated data

The use of modular processing systems and service capabilities using the real or near real-time data provided by the EDW solution, applying consistent business rules will reshape the application landscape, reducing duplicated applications and inconsistent processing. The implementation of Modular Systems Future State will:

- Retain and improve mature working operational business processing capabilities
- Standardize business processing (e.g., enrollment, case management) to improve recipient and provider experience
- Add new processing capabilities without the capacity constraints of a single vendor
- Enable use of processing services by external organizations and systems
- Enable high quality and accessible data
- Improve integration with external partners

- Reduce complexity
- Improve healthcare outcomes
- Enable holistic decision-making
- Use evidence-based processing

The PMM is associated with tangible and intangible benefits across all FX Guiding Principles with an emphasis on the following:

- Reduce complexity / enable high-quality and accessible data (intangible)
 - › The PMM will be a single data source to be used and shared among agencies and AHCA divisions to limit the need for redundant information to be supplied by the provider. Automated edits will be built into the portal to enhance the quality of data upon submission.
- Improve integration with partners
 - › The PMM will streamline and simplify provider licensure (DOH), facility licensure (AHCA HQA), Medicaid enrollment (AHCA MFAO), plan credentialing, and account management processes.
- Improve provider and recipient experience
 - › The PMM will improve provider experience with entities in the Medicaid Enterprise by reducing the time necessary to participate in Medicaid, the number of entities to which providers supply the same information, and the amount of time providers spend on administration (intangible and indirect).
- Improve healthcare outcomes (intangible)
 - › The PMM is expected to increase healthcare outcomes in the long-term by increasing access to care for recipients (i.e., the number of providers and specialties) as participating in Medicaid carries less administrative constraints and the Agency's ability to monitor network adequacy.

7.1.2 ORGANIZATIONAL IMPACTS

The implementation of improved technologies will enable organizational change to improve the delivery of healthcare services. The foundational technologies and improved systems will reduce duplication, data inconsistency and processing delays. Within the Medicaid Enterprise, agencies reorganization, restructure, and consolidation will be possible to optimize business agility and service delivery. External to State agencies, healthcare providers and health plans may change organizational size and structure following improvements in efficiency and increased use of data for coordination of care. Specific future impacts are unknown. Anticipated changes include:

- Consolidation of policy administration and policy implementation within systems
- Consolidation of recipient, provider, and health plan interaction center (e.g., call center) operations

- A hybrid vertical and horizontal segmentation of service delivery by delivery model, claim type, advanced payment model, or recipient categorization

7.1.3 RISKS

The purpose of risk management is to address project risk in a controlled and intentional manner to realize the anticipated value of the project while balancing risk and reward. Formal risk management aims to identify and manage risks that are not addressed by other project management processes.

The FX Project Management Standards, outlines the processes used to identify, analyze, plan responses, and monitor and control risks associated with the project. The process will facilitate the development of action plans to reduce the probability of occurrence and contingency plans as appropriate to minimize the impact of a realized risk event on the project.

To be successful, risk management must be an ongoing process throughout the life of the project. The process begins with identifying and assessing significant risks, then developing appropriate response plans. It continues with regular risk monitoring, ongoing new risk identification, and timely plan implementation. Risks are communicated through the management structure as defined by the escalation process. As part of the risk response plan, the Risk Owner will determine which additional project stakeholders should be aware of potential risks throughout the project life cycle.

The following set of key principles will guide the Risk Management Processes for the project:

- A risk has a cause, and if it eventually occurs, a consequence. As such, a risk is an uncertain event or condition which if it occurs, may result in a negative impact on the project objectives. Risk management is the systematic process of identifying, assessing, responding, and controlling risks
- The probability of success for any project can be significantly increased through a formal, proactive, and iterative risk management approach. It is important risks are quickly identified, and appropriate steps are taken to address them
- Risk management is an iterative process which needs to occur throughout the project. As the project progresses, the project team becomes more knowledgeable and better equipped to identify and manage project risks. Additionally, risks evolve and change

Identification of risk must occur at every level of the organization. All project team members should be able to recognize risks during their daily work and should bring potential risks to the attention of their team leaders or managers. Project teams shall identify and capture individual risks and sources of overall risk to facilitate the successful management of risks. Risk identification is an ongoing process throughout the life of the project.

Utilizing the Project Charter, draft schedule, other project documents, and the Risk Breakdown Structure guide as inputs, project teams shall conduct an initial risk identification session(s). Project teams shall use these sessions to identify and evaluate potential events that could positively or negatively impact the project, develop response plans, and manage accordingly. The Project Manager (or designee) shall add identified risks to the Risk Log located in the FX Projects Repository.

The FX Enterprise Program Management Office (EPMO) is alerted when the Risk Log is modified and shall verify and validate new risks. In the case of risks that specify impact or dependency on other FX projects the FX EPMO shall work with the project teams to draft an appropriate risk response.

7.1.3.1 PERFORM RISK ASSESSMENT

Project teams shall facilitate risk assessments with the intent of developing a risk response plan based on the risk's exposure to the project. Project teams shall evaluate the risk's probability of occurring and the impact the risk would have, as well as what the triggering point could be.

7.1.3.2 EVALUATING PROBABILITY OF OCCURRENCE

FX project teams shall use the matrix in **Table 10: Probability of Occurrence** to assess the *Probability* field of the risk form.

Probability	Likelihood of Occurring	Numeric Value
Low	Unlikely	1
Medium	Likely	3
High	Very Likely	5

Table 10: Probability of Occurrence

Project teams in the ongoing assessment of risks in relation to other project risks, events, or activities should consider whether the associated triggering event is imminent (less than approximately eight weeks) when evaluating probability of the risk to be triggered.

7.1.3.3 ASSESSING RISK IMPACT

Project teams shall use the matrix in **Table 11: Impact on Projects**

to assess the impact to cost, schedule, scope, and quality of a potential risk event.

Impact	Dimensions to Consider				Numeric Value
	Cost	Schedule	Scope	Quality	
Low	Impact to cost is below appropriation	No or little impact to project schedule	Minor clarification to existing scope	Project quality is not in jeopardy	1
Medium	Impact to cost is above appropriation by less than 10%	Schedule impact is possible	Scope change is noticeable, but not deemed significant	Impact to quality possible	3
High	Impact to cost is above appropriation by greater than 10%	There is significant impact to Schedule and deliverable due dates	There is a significant change in Scope	Impact to quality is very likely	5

Table 11: Impact on Projects

The impact of a risk related to multiple factors will likely be the average of all relevant factors.

7.1.3.4 CALCULATING THE RISK EXPOSURE SCORE

The final step in the qualitative risk analysis process is to update the Risk Form with the probability and impact values captured in the previous two steps. Computation of the risk exposure value is automatic within the Risk Log based upon the probability and impact values entered. The formula used for the calculation is as follows:

Risk Exposure Score = Impact value x Probability value

The risk exposure score supports making further decisions in the response planning processes. Risks with risk score values 15 or greater are considered having high exposure.

Table 12: Calculated Risk Exposure provides an example of the Risk Exposure Scoring.

Risk Score		Probability		
		1 - Low	3 - Medium	5 - High
Impact	1 - Low	1	3	5
	3 - Medium	3	9	15
	5 - High	5	15	25

Table 12: Calculated Risk Exposure

If a risk has a risk exposure score of 15 or higher, FX EPMO shall monitor the risk along with any risk that has a potential for impact on another FX Project. The project team, FX EPMO, and the Agency will collaboratively monitor risks that fall into this category.

7.1.3.5 PLAN RISK RESPONSES

The project team shall prioritize any risk identified as *very likely* or with *most significant impact* with imminent timelines. Responses shall be provided for all risks and then the project team shall then develop strategies (response plans and contingency plans) for those project prioritized risks. Project teams shall determine the required activities and resources to address the risks.

Risk Responses:

- **Risk Acceptance** – Assumes the potential risk as unavoidable with acceptable impact given project contingencies in terms of budget or schedule that allow project teams to continue the project without further consideration
- **Risk Avoidance** – Avoid the risk by eliminating the cause of the risk, the consequence of the risk, or both (e.g., forego certain aspects of the project which are particularly risky)
- **Risk Mitigation** – Manage risk by developing a risk response plan which prioritizes, implements, and maintains controls by either significantly reducing the likelihood or impact of the triggering event
- **Risk Transference** – Transfer or share risk through options which compensate for the adverse impact, such as performance bonding and insurance

The risk response may require project documents (i.e., PMP, project schedule) be updated. If there is impact to the schedule, scope, or cost the project team should assess the need for a Project Change Request. The risk response and contingency planning will be updated in the FX Projects Repository.

7.1.4 MONITORING AND CONTROLLING RISK

Project teams shall continually perform risk identification, risk response planning, and risk monitoring through the life of the project. Project teams shall track and report on those risks that have been identified as high exposure (15+) or with imminent trigger dates (less than eight weeks out). Risk owners are responsible in providing updates to the project manager in a timely manner for addressing responses and reporting to key stakeholders. In accordance with administrative rule, the FX EPMO shall compile and report high exposure risks to the Department of Management Services (DMS) in the required Monthly Status Report.

Project teams shall review new risks and risks with exposures of 15+ during project status meetings. Project managers shall review all project risks monthly, and report risk information weekly and monthly as detailed in the communication plan. Project teams may also discuss risks which require status updates, imminent risk triggering event dates, and those with upcoming response activity in regularly scheduled project risk meetings

The FX EPMO shall monitor all project risks to assess overall riskiness of the program and collaboratively control risks that affect multiple projects. The FX EPMO Lead (or designee) facilitates program-level risk meetings and uses those meetings to discuss program-level risks, new project-level risks, and high probability/high impact project-level risks.

Table 13: Risk Management Activities lists the key project Risk Management activities.

ACTIVITY	APPROACH	PURPOSE
1 Identify Risk	<ul style="list-style-type: none"> ▪ Create a list of project risks; gather risks from stakeholders using brainstorming, predefined lists, and/or completion of risk form 	<ul style="list-style-type: none"> ▪ Identifies project risks before they become problems; helps to set expectations and provide a vehicle for reaching consensus – unknown risks cannot be managed
2 Validate Risk	<ul style="list-style-type: none"> ▪ Discuss all newly identified risks with the SEAS Project Risk Team, SEAS Director, FX Director, and affected stakeholders to establish credibility of the risk 	<ul style="list-style-type: none"> ▪ To ensure the information is complete, the identified risk is valid and not a duplicate
3 Log Risk	<ul style="list-style-type: none"> ▪ Log the risk in the Risk Log located on the FX Projects Repository 	<ul style="list-style-type: none"> ▪ To ensure the risk is thoroughly documented
4 Perform Risk Analysis	<ul style="list-style-type: none"> ▪ Determine the consequence of risks listed (probability and impact) and calculate the risk tolerance 	<ul style="list-style-type: none"> ▪ Transforms the risk data into decision-making information
5 Formulate Risk Response Plan	<ul style="list-style-type: none"> ▪ Determine desired risk strategies and actions, and assign responsibility 	<ul style="list-style-type: none"> ▪ Translates the risk information into strategies and mitigation actions
6 Approve Risk Response Plan	<ul style="list-style-type: none"> ▪ Gather consensus on risk strategies and actions, and approve their assignment to an owner(s) 	<ul style="list-style-type: none"> ▪ Assigns accountability to Risk Owner
7 Execute Risk Response Plan	<ul style="list-style-type: none"> ▪ Mobilize action plans 	<ul style="list-style-type: none"> ▪ Risk response actions are executed such that the probability of the risk occurring, and the impacts are minimized
8 Monitor Risk	<ul style="list-style-type: none"> ▪ Review and re-examine risks when the project situation changes or key milestones are achieved. Discuss and review project risks and plans in project status, or other scheduled meetings, when the project situation changes or key milestones are achieved 	<ul style="list-style-type: none"> ▪ Monitors risk indicators and risk response actions

ACTIVITY	APPROACH	PURPOSE
9 Close Risk	<ul style="list-style-type: none"> ▪ As part of risk monitoring, when the SEAS Project Risk Team, SEAS Director, or FX Director agrees the risk can no longer occur, the probability of the risk will be changed to zero and the status will be set to <i>Closed</i> 	<ul style="list-style-type: none"> ▪ Enables the SEAS Project Risk Team to remain focused on active risks which have a potential to affect the project

Table 13: Risk Management Activities

Risks to the project reflect risks to the FX solution and any additional risks identified in the future will be incorporated into the complete list of project risks. The current list of project risks can be found at in the FX Projects Repository under FX Risk Log.

7.1.5 ISSUES TO RESOLVE

Risks may develop into Issues and ultimately result in Action Items which will provide resolution. Disciplined management of Issues and Action Items enables a project team to effectively resolve the issues and complete action items promptly and keep a project on track. A formal Issue / Action Item Management process provides the mechanism throughout the life cycle of the project to bring issues and action items to resolution.

- **Issue** - An Issue is an existing constraint negatively impacting project timeliness, quality, resources, or cost. Issues requiring attention from another level or area within the project governance structure will be subject to the formal issue escalation process.
- **Action Item** - An Action is a proactive task identified by the SEAS Project Team to address a known problem or situation. Actions may also come from a risk or issue item. Incomplete or overdue action items may create issues.

Issues often arise from risks that have reached their trigger event without successful mitigation or avoidance and are causing disruption to the project activity. A project manager shall conduct a root cause analysis to determine cause, and work with the project team and Agency Project Sponsor to identify and employ a reasonable resolution strategy. Any impact to scope, schedule, or cost should be assessed, and change managed accordingly.

The project manager is responsible for monitoring issues identified during the project and driving their resolution. Issue resolution activities are conveyed during project status meetings and program-level risk and issue meetings.

If the project team cannot resolve an issue in a timely manner, the project manager should consult with the Agency Project Sponsor and subsequently the FX EP MO. The FX EP MO shall coordinate the issue escalation process with the SEAS Governance Team. The FX EP MO shall collaboratively address issues that impact multiple projects or components on the FX Portfolio Roadmap.

An issue may be identified in any number of ways. For example:

- A problem which is negatively impacting the project for which there is no apparent answer
- A current situation or event which could or is negatively impacting the project and cannot be answered immediately but requires some research and analysis to provide insight into actions which should be taken
- An inability of two project entities or functional groups to come to an agreement on an item or process
- An Action Item with a late due date which, if not completed, will negatively impact the project
- The need for information external to the project inhibits or stops the development of the project objectives, deliverables, and/or solution until resolved
- A trigger, as defined in the Risk Log, has been activated for a currently identified risk

If an issue is significant and an impact analysis reveals the resolution would impact cost, scope, or the schedule critical path, then the issue should be escalated according to the escalation process defined in the FX Project Management Standards. The current list of issues can be found in the FX Projects Repository under FX Issue Log.

7.1.6 CRITICAL SUCCESS FACTORS FOR REMAINDER OF PROJECT

Table 14: Critical Success Factors outlines the factors and criteria to measure the success of the modular implementation approach.

#	Description of Success Factors	How will the Criteria be measured/assessed?
1	Completion of CMS milestone reviews throughout the Medicaid Enterprise Certification Life Cycle using the current Medicaid Enterprise Certification Toolkit (MECT), achievement of CMS certification for Medicaid Enterprise System, and approval for enhanced FFP.	Measured and assessed by CMS through the CMS-prescribed certification process
2	Architecture enables enhanced data: integrity, reliability, single source of truth, availability in real-time, analytics, and analysis.	Assessed by the SEAS management team and designated Agency Subject Matter Experts
3	Enhanced Provider Experience improving all areas where the provider interacts with the Agency, which will include the following: enrollment, claims process, and reimbursement, among others.	Assessed by the SEAS management team and designated Agency Subject Matter Experts
4	Improved Program Integrity which provides the Agency the ability to more accurately identify improper payments and discrepancies.	Assessed by the SEAS management team and designated Agency Subject Matter Experts
5	Improved Recipient Experience and Health Outcomes.	Measured through Healthcare Effectiveness Data and Information

		Set (HEDIS) and Consumer Assessment of Healthcare Providers and Systems (CAHPS) quality indicators
6	Successful completion of the design, development, and implementation (DDI) of the IS/IP vendor’s solution.	Assessed by the SEAS Management Team and designated Agency Subject Matter Experts
7	Successful procurement of the EDW vendor and initiation of design and development of the vendor’s solution.	Assessed by the SEAS Management Team and designated Agency Subject Matter Experts
8	Successful completion of the design, development, and implementation (DDI) of the EDW vendor’s solution.	Assessed by the SEAS Management Team and designated Agency Subject Matter Experts
9	Successful development of CMS-approved requirements for the Provider Management module procurement.	Assessed by the SEAS Management Team and designated Agency Subject Matter Experts
10	Successful procurement, including the development of CMS-approved requirements, of the Provider Management module vendor and initiation of design and development of the vendor’s solution.	Assessed by the SEAS Management Team and designated Agency Subject Matter Experts
11	Successful completion of the design, development, and implementation (DDI) of the Provider module vendor’s solution.	Assessed by the SEAS Management Team and designated Agency Subject Matter Experts

Table 14: Critical Success Factors

SECTION 8 GLOSSARY

Term / Acronym	Definition
AES	Advanced Encryption Standards
Agency	Florida Agency for Health Care Administration
AHCA	Florida Agency for Health Care Administration
AHS	Automated Health Solutions
APD	Agency for Persons with Disabilities
API	Application Programming Interface
ASR	Application Service Registry
BUR	Backup and Restore
CAHPS	Consumer Assessment of Healthcare Providers and Systems
C-COTS	Claims Complaint Oversight System
CDM	Conceptual Data Model
CHCUP	Child Health Checkup
CIRTS	Client Information and Registration Tracking System
CMS	Centers for Medicare and Medicaid Services
CM	Content Management
COTS	Commercial-Off-The-Shelf
CPBSC	Care Provider Background Screening Clearinghouse
DCF	Department of Children and Families
DFS	Department of Financial Services
DJJ	Department of Juvenile Justice
DOEA	Department of Elder Affairs
DOH	Department of Health
DRG	Diagnosis Related Grouping
DSS	Decision Support System
EAPG	Enhanced Ambulatory Patient Grouping
ECDM	Enterprise Conceptual Data Model
EDI	Electronic Data Interchange
EDW	Enterprise Data Warehouse
EPMO	Enterprise Program Management Office
ESB	Enterprise Service Bus
ETL	Extract Transform Load
EVV	Electronic Visit Verification
FCS	Florida Cybersecurity Standards
FDLE	Florida Department of Law Enforcement
FFM	Federally Facilitated Marketplace
FFP	Federal Financial Participation
FFS	Fee for Service
FHA	Federal Health Architecture
FHCTR	Fair Hearing Case Tracking and Reporting
FHIM	Federal Health Information Model

FHIR	Fast Healthcare Interoperability Resources
FHKC	Florida Healthy Kids Corporation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act or Federal Information Security Modernization Act
FMMIS	Florida Medicaid Management Information System
FTP	File Transfer Protocol
FX	Florida Health Care Connection
HEDIS	Healthcare Effectiveness Data and Information Set
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HL7 RIM	Health Level 7 Reference Information Model
HQA	Health Quality Assurance
IS/IP	Integration Services and Integration Platform
IT	Information Technology
ITN	Invitation to Negotiate
IV&V	Independent Verification and Validation
IVR	Interactive Voice Response
LBR	Legislative Budget Request
MCST	Managed Care Survey Tool
MDM	Master Data Management
MECT	Medicaid Enterprise Certification Toolkit
MES	Medicaid Enterprise System
MFA	Medicaid Fiscal Agent
MFAO	Medicaid Fiscal Agent Operations
MFCU-OAG	Medicaid Fraud Control Unit - Office of the Attorney General
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MOI	Master Organization Index
MPI	Master Person Index
MPR	Medicaid Enterprise Project Repository
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NwHIN	Nationwide Health Information Network
ODS	Operational Data Store
ONC	Office of National Coordinator for Health Information Technology
PA	Prior Authorization
PBM	Pharmacy Benefit Management
PBMS	Prescription Benefit Management System
PHI	Protected Health Information
PII	Personal Identifying Information
PMO	Project Management Office and Program Management Office
PNV	Provider Network Verification

POAR	Persona Optimized Analytics and Reporting
POS	Point of Sale
QA	Quality Assurance
RDS	Reporting Data Store
RHIO	Regional Health Information Organizations
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDS	Specialized Data Store
SEAS	Strategic Enterprise Advisory Services
SFTP	Secured File Transfer Protocol
SME	Service Management Engine
SMMC	Statewide Medicaid Managed Care
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SQL	Structured Query Language
SS-A	MITA State Self-Assessment
SSL	Secure Socket Layers
SSO	Single Sign-On
SSOT	Single Source of Truth
TCO	Total Cost of Ownership
TPL	Third Party Liability
TSRG	Technology Standards Reference Guide
UI	User Interface
VPN	Virtual Private Network
WS	Web Services
XML	Extensible Markup Language

SECTION 9 APPENDICES

[Appendix A – Supporting Artifacts](#)

[Appendix B – Technology Deliverables](#)

[Appendix C – Technology Standards](#)

[Appendix D – Inbound and Outbound Interfaces](#)

APPENDIX A: SUPPORTING ARTIFACTS

Supporting Artifacts	Links to Source Document
Florida MES Procurement Strategy	Florida MES Procurement Strategy
Approved Planning Advanced Planning Document (PAPDU)	PAPDU - April 2019
EDW Project Partnership Understanding	EDW PPU
P-1: MITA State Self-Assessment and Update Process	2019 MITA SSA
P-2: FX Project Management Standards	P-2: FX Project Management Standards
S-3: Enterprise Systems Strategic Plan and Refresh	S-3 Enterprise Strategic Plan 2020 S-3 Refresh 2020 Refresh Appendix
S-4: Strategic Project Portfolio Management Plan	S-4: Strategic Portfolio Management Plan
MITA Concept of Operations and Addendum	MITA Con Ops 2020 MITA Con Ops Addendum
Integration Services and Integration Platform Invitation to Negotiate Enterprise Data Warehouse Invitation to Negotiate Provider Management Module Business Case Schedule IV-B FY 20/21	Posted IS/IP ITN Posted EDW ITN PMM Business Case Schedule IV-B FY 20-21

APPENDIX B: TECHNOLOGY DELIVERABLES

Technology Deliverable	Link to Source Document
T-1 Data Management Strategy	T-1: Data Management Strategy
T-2 Information Architecture	T-2: Information Architecture
T-3 Data Standards	T-3: Data Standards
T-4 Technical Management Strategy	T-4: Technical Management Strategy
T-5 Technical Architecture	T-5: Technical Architecture
T-6 Technology Standards	T-6: Technology Standards
T-7 Design Implementation Management Strategy	T-7: Design Implementation Management Strategy
T-8 Enterprise Data Security	T-8: Enterprise Data Security

APPENDIX C: TECHNOLOGY STANDARDS

Category	Standard Name	Objective	Link to Source Document
Project Documentation	Florida Information Technology Project Management and Oversight Standards	This is DMS Administrative Rule 60GG-1 which establishes project management standards when implementing information technology (IT) projects. State Agencies must comply with these standards when implementing all IT projects. Cabinet Agencies must comply with these standards when implementing IT projects that have a total cost of \$25 million or more and that impact one or more other agencies (pursuant to section 282.0051(13)(a), F.S.). For all other IT projects, Cabinet Agencies are required to either adopt these standards or adopt alternative standards based on best practices and industry standards (section 282.00515, F.S.). These standards are documented in Rule 60GG-1.001 through 60GG-1.008, F.A.C.	Florida IT DMS Rule 60GG-1
Design	Business Process and Rules Management Plan	The Business Process and Rules Management Plan provides the processes for managing the business requirements, business rules, user requirements, and functional / nonfunctional requirements for the project. It may also contain use case scenarios to help clarify the process required for the project.	FX Business Process and Rules Management Plan Template
Requirements	Requirements Management Plan	This Integrated System Requirements Management Plan (RM Plan) describes in detail the system requirements, including the vision, global design requirements, and business requirements for guidance and use during the development of the FX <project name>.	FX Requirements Management Plan Template
Design	Systems Impact Analysis Management Plan	The Systems Impact Analysis Management Plan is to communicate all possible inputs and outputs from the system for all potential actions whether they are internal to the system or transparent to system	FX Systems Impact Analysis Management Plan Template

		users. This plan helps ensure compatibility between system segments and components.	
Development	Configuration Management Plan	This Configuration Management (CM) Plan establishes the technical and administrative direction and surveillance for the management of configuration items (i.e., software, hardware, and documentation) associated with the <Project Name (Acronym)> that are to be placed under configuration control.	FX Configuration Management Plan Template
Requirements	(System) Change Management Plan	Provide a high-level overview of the project and a description of how the <Project Name> change management activities are processed in accordance with the Integrated Change Control Process defined in the FX P2: Project Management Plan, specifically the Interim PMO – Scope Change Management Plan.	FX Change Management Plan Template
Testing	Testing Management Plan	The Testing Management Plan describes the overall technical and management approach, resources, and schedule for all intended test activities associated with development, validation, implementation, and operational testing.	FX Testing Management Plan Template
Maintenance	Software Problem Resolution Standards and Procedures Plan	This Software Problem Resolution Standards and Procedures Plan (SPR Plan) describes the approach for continued software development process improvement during the life cycle of the <Project Name (Acronym)>. The document identifies the specific actions that will be taken to improve the software process and outlines the plans for implementing those actions.	FX Software Problem Resolution Standards and Procedures Plan Template
Maintenance	Integrated System Implementation Management Plan	This Integrated System Implementation Management Plan (IM Plan) describes how the automated system/application or IT situation will be installed, deployed, and transitioned into an operational system or situation.	FX Integrated System Implementation Management Plan Template

Maintenance	Integrated Program Operations and Maintenance Planning/Deployment Plan	The Integrated Program Operations and Maintenance Planning/Deployment Plan (O&M Plan) is the guide for those who maintain, support, and/or use the system in a day-to-day operations environment.	FX Integrated Program Operations and Maintenance Planning/Deployment Plan Template
Maintenance	Post Implementation Evaluation Plan	The Post Implementation Evaluation Plan is an internal evaluation to confirm that a system is operating according to design and that users are satisfied with the performance of the system. This plan represents the transition from design and implementation stage to the operations stage and signals the start of monitoring metrics established for the system.	FX Post Implementation Evaluation Plan Template
Testing	Quality Management Plan	The Quality Management Plan documents the necessary information for planning, managing, and controlling project and product quality to meet FX objectives. It defines the project's quality policies, procedures, areas of application and associated criteria, and roles and responsibilities.	FX Quality Management Plan Template
Maintenance	CMS Contingency Planning Standards	CMS is reliant on its information systems for mission fulfillment. Information systems are susceptible to a wide variety of events and threats that may affect their ability to process, store, and transmit raw data and information. Contingency planning is one method of reducing risk to CMS' operations by providing prioritized, efficient, and cost-effective recovery strategies and procedures for the organizations' Information Technology (IT) infrastructure. The CMS Contingency Planning Standard is consistent with the guidance of NIST and most specifically with NIST Special Publication (SP) 800-34 revision 1, <i>Contingency Planning Guide for Federal Information Systems</i> ² dated May 2010. Effective contingency planning requires clear and concise:	CMS Contingency Planning Standard

		<ul style="list-style-type: none"> · Disaster declaration criteria · Recovery prioritization <p>These, in turn, require:</p> <ul style="list-style-type: none"> · Accurate identification of functions performed by the system · Accurately mapping any functions that rely on other systems · Determining impact to the organization for loss of any or all functions (and thereby determine functional recovery prioritization) 	
Maintenance	Disaster Recovery Plan	The Disaster Recovery (DR) Plan provides step-by-step procedures to identify, address, and recover from disaster events. It also emphasizes the need to minimize negative impacts to the project and resume normal operations.	FX Disaster Recovery Plan Template
Maintenance	NIST IT Contingency Planning Guide	NIST Special Publication 800-34, Rev. 1, <i>Contingency Planning Guide for Federal Information Systems</i> , provides instructions, recommendations, and considerations for federal information system contingency planning. Contingency planning refers to interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods. This guide addresses specific contingency planning recommendations for three platform types and provides strategies and techniques common to all systems. This guide defines a seven-step contingency planning process that an organization may apply to develop and maintain a viable contingency planning program for their information systems.	NIST SP 800-34, Revision 1

Architecture, Analysis and Design Standards	Database Naming Standards	These are the database naming standards of the MMIS system.	Database Naming Standard
Architecture, Analysis and Design Standards	Reporting Implementation Procedures	The purpose of this document is to identify and communicate the report promotion procedures within the Agency to achieve data validity, security, efficiency, and conformity.	Reporting Standards
Architecture, Analysis and Design Standards	Continuity of Care Record (CCR)	CCR is a core data set of relevant administrative, demographic, and clinical information facts about a patient’s health care, covering one or more encounters. It provides a communication method between practitioner, system, or setting and aggregates the pertinent data. There are three core components, the CCR Header, the CCR Body, and the CCR Footer.	Continuity of Care Record Standard
Data Standards	Current Dental Terminology (CDT)	CDT is a code set with descriptive terms developed and updated by the American Dental Association (ADA) for reporting dental services and procedures to dental benefits plans.	Dental Terminology Code Set
Architecture, Analysis and Design Standards	Digital Imaging Communications in Medicine (DICOM)	DICOM standards enable stakeholders to retrieve images and associated diagnostic information, transfer them from various manufacturers’ devices and medical workstations.	DICOM Standards
Architecture, Analysis and Design Standards	Logical Observation Identifiers Names and Codes (LOINC)	LOINC is a database and universal standard for identifying medical laboratory observations, developed and maintained by the Regenstrief Institute. The creation of LOINC was in response to the demand for an electronic database for clinical care and management. It is publicly available at no cost.	LOINC Standards
Architecture, Analysis and Design Standards	Public Health Information Network (PHIN)	PHIN is a national initiative to increase the capacity of public health agencies to electronically exchange data and information across organizations and jurisdictions.	PHIN

Architecture, Analysis and Design Standards	Systematized Nomenclature of Medicine – Clinical Terms (SNOMED CT)	This is the most comprehensive set of multilingual clinical healthcare terminology. Its aim is to improve patient care through the development of standardized clinical terminology regardless of language.	SNOMED CT
Architecture, Analysis and Design Standards	Unified Medical Language System (UMLS)	This is a set of files and software collections from health and biomedical vocabularies and standards to enable interoperability between systems.	UMLS Standards
Service Interoperability	Open Data Protocol (OData)	OData is an open protocol to allow the creation and consumption of quarriable and interoperable RESTful APIs in a simple and standard way.	OData Standards
Data Standards	Current Procedural Terminology, Fourth Edition (CPT-4)	A listing of descriptive terms and identifying codes for reporting medical services and procedures. Covers physician services, physical therapy, occupational therapy, radiology, medical diagnostic procedures, hearing, vision, and medical transportation.	CPT-4 Standards
Data Standards	Diagnosis Related Group (DRG)	System to classify hospital cases into groups expected to have similar hospital resource use.	DRG
Data Standards	Healthcare Common Procedure Coding System (HCPCS)	Set of healthcare procedure codes based on the American Medical Association's Current Procedural Terminology (CPT) which are used to provide healthcare claims that are managed consistently and in an orderly manner.	HCPCS
Data Standards	ICD-10	The 10th revision of a medical classification list by the World Health Organization (WHO) which contains codes for diseases, signs and symptoms, abnormal findings, complaints, social circumstances, and external causes of injury or diseases.	ICD-10

Data Standards	National Drug Codes (NDC)	The NDC is a unique product identifier used in the United States for drugs intended for human use. The Drug Listing Act of 1972 requires registered drug establishments to provide the Food and Drug Administration (FDA) with a current list of all drugs manufactured, prepared, propagated, compounded, or processed by it for commercial distribution.	NDC
Data Standards	Global Trade Identification Number (GTN)	GTN is an identifier for trade items, developed by GS1, used to look up product information in a database which may belong to a retailer, manufacturer, collector, researcher, or other entity.	GTN
Data Standards	Health Industry Bar Code – Labeler Identification Code (HIBC-LIC)	Establishes and maintains unique identifiers and labeling standards for medical equipment, supplies, and devices.	HIBC-LIC
Data Standards	Arden Syntax	The Arden Syntax is a formalism for representing procedural clinical knowledge to facilitate the sharing of computerized health knowledge bases among personnel, information systems, and institutions.	Arden Syntax
Data Standards	Clinical Context Object Workgroup, Management Specification (CCOW)	HL7 standard protocol designed to enable disparate applications to synchronize in real time, and at the user-interface level. CCOW serves as the basis for ensuring secure and consistent access to patient information from heterogeneous sources.	CCOW
Data Standards	Clinical Document Architecture (CDA)	HL7 XML-based markup standard intended to specify the encoding, structure, and semantics of clinical documents for exchange.	CDA
Data Standards	IEEE 1073	Medical / health device communication standards enable communication between medical, healthcare, and wellness devices and with external computer systems.	IEEE 1073

Data Standards	Abstract Syntax Notation One (ASN.1)	Data syntax and constraint language that describes rules and structures for representing, encoding, transmitting, and decoding data in telecommunications and computer networking.	ASN.1
Data Standards	ebXML Business Process Specification Schema (BPSS)	ebXML specification schema provides a standard framework to configure business systems to support business transactions.	ebXML BPSS
Data Standards	ebXML Collaboration-Protocol Profile and Agreement Specification	Standard for two or more business partners to engage in business transactions based on each party's message exchange capabilities as described in a Collaboration Protocol Profile (CPP) and agreed to in a Collaboration Protocol Agreement (CPA).	ebXML Collaboration-Protocol
Data Standards	ebXML Message Service Specification (EbMS)	Defines the message envelope and header schema used to transfer ebXML messages over a communications protocol (e.g., HTTP or SMTP) and the behavior of software sending and receiving ebXML messages.	EbMS
Data Standards	International Organization for Standardization: Information Technology — Metadata Repository Standard (ISO 11179)	ANSI standard that supports registration of data regardless of syntax, naming, definition conventions, and registry interoperability.	ISO 11179
Data Standards	International Organization for Standardization: Protocol for Information Search and Retrieval (ISO 23950)	Standard client–server, application layer communications protocol for searching and retrieving information from a database over a TCP/IP computer network.	ISO 23950
Data Standards	Object Constraint Language (OCL)	UML-based standard for specifying the refinements of artifacts based on models that are essential for documenting collaboration profiles.	OCL Standards

Data Standards	Federal Health Information Model (FHIM)	A model of healthcare data developed for the FHA partner agencies seeking to develop a common Logical Information Model or Computationally Independent Model (CIM).	FHIM Standards
Data Standards	X12 Companion Guide (834)	Companion Guide for ASC X12 Benefit Enrollment and Maintenance (834) transaction type.	X12 834 Companion Guide
Data Standards	X12 Companion Guide (837P)	Companion Guide for ASC X12 Professional Health Care Claim (837P) transaction type.	X12 837P Companion Guide
Data Standards	X12 Companion Guide (278)	Companion Guide for ASC X12 Health Care Services Review (278) transaction type.	X12 278 Companion Guide
Data Standards	X12 Companion Guide (835)	Companion Guide for ASC X12 Health Care Claim Payment and Remittance (835) transaction type.	X12 835 Companion Guide
Data Standards	X12 Companion Guide (837I)	Companion Guide for ASC X12 Institutional Health Care Claim (837I) transaction type.	X12 837I Companion Guide
Data Standards	X12 Companion Guide (837D)	Companion Guide for ASC X12 Dental Health Care Claim (837D) transaction type.	X12 837D Companion Guide
Data Standards	X12 Companion Guide (820)	Companion Guide for ASC X12 Health Care Premium Payment (820) transaction type.	X12 820 Companion Guide
Data Standards	X12 Companion Guide (277U)	Companion Guide for ASC X12 Health Care Payer Unsolicited Claim Status (277U) transaction type.	X12 277U Companion Guide
Data Standards	X12 Companion Guide (276/277)	Companion Guide for ASC X12 Health Care Claim Status Request and Response (276/277) transaction type.	X12 276/277 Companion Guide
Data Standards	X12 Companion Guide (270/271)	Companion Guide for ASC X12 Health Care Eligibility Inquiry and Response (270/271) transaction type.	X12 270/271 Companion Guide
Data Standards	Database Object Naming	Centers for Medicare & Medicaid Services (CMS) standard for database object naming.	CMS Database Object Naming Standards
Data Standards	UML Modeling	UML Modeling Specification for the design of persistent data.	UML Modeling Specification Version 2.5.1

Data Standards	Web Services Metadata Exchange	Specification that defines how metadata associated with a web service can be represented as WS-Transfer resources or HTTP resources, how metadata can be embedded in WS-Addressing endpoint references, how metadata could be retrieved from a metadata resource, and how metadata associated with implicit features can be advertised.	Web Services Metadata Exchange
Data Standards	International Organization for Standardization: Information Technology — Statistical Data and Metadata Exchange Standard (ISO 17369)	ANSI standard that provides an integrated approach to facilitating Statistical Data and Metadata Exchange (SDMX), enabling interoperable implementations within and between systems concerned with the exchange, reporting, and dissemination of statistical data and related metadata.	ISO 17369
Business Enabling Technologies	Data Visualization Tool	Tableau is the AHCA tool standard for data visualization.	Tableau Data Visualization Tool
Data Standards	Data Archiving	Standards for the archival and storage of data in any form (e.g., electronic, paper).	
Data Standards	Data Purging Standards	Standards for the permanent destruction of data in any form (e.g., electronic, paper).	
Data Standards	Records Retention	Standards for the retention of information in any form (e.g., electronic, paper).	
Data Standards	Data Standards for Eligibility	Data format standards for eligibility (e.g., always keep first data instance).	
Data Standards	Record Locking Patterns	Standard patterns for record locking (e.g., original value, time stamping).	
Architecture, Analysis and Design Standards	Information Logging	Standards for information logging across application portfolios including log categorization and archiving of logs.	
Architecture, Analysis and Design Standards	Code Repository Management	Standards for how code is managed in the code repository including patterns for check in, check out, labeling, branching, and merging.	

Architecture, Analysis and Design Standards	Service Versioning	Standards and patterns for how services are versioned.	
Data Standards	Data Monetization	Standards for generating measurable economic benefit from available data sources.	
Data Standards	Geographic Information System (GIS) Data Standards	Standards for the collection, storage, and use of Global Information System (GIS) data.	
Data Standards	Data Ownership Standards	Standards for data ownership.	
Data Standards	Content Management Data Storage	Standards for content management storage.	
Data Standards	Data Normalization	Standards for the normalization of data.	
Data Standards	Metadata Standards	Standards for the level of granularity and storage of metadata.	
Data Standards	Data Redaction	Data redaction standards for the protection of sensitive information.	
Data Standards	Records Retention	General Records Schedule GS-1 for State and Local Government.	Florida DOS General Records Schedule GS1-SL
Data Standards	Records Retention	Records Retention schedule of the Centers for Medicare and Medicaid Services (CMS).	CMS Records Retention Guidance
Project Documentation	Document Naming Standards	USGS S&L Medicaid Implementation Services Documentation Procedures and Standards How to Document FL MMIS	USGS S&L MMIS Documentation Procedures and Naming Standards
Security and Privacy	Liberty Alliance – Federated Approach	Federated network identity is the key to reducing the friction between the need to share, the desire for autonomy, and the need for clear identity without centralized control. A federated network identity model will ensure that appropriate parties use critical private information. Liberty Identity Federation Framework (ID-FF) offers a viable approach for implementing such as single sign-on and federated identities.	Project Liberty

<p>Security and Privacy</p>	<p>Security Assertion Markup Language (SAML)</p>	<p>SAML defines a framework for exchanging security information between online business partners. SAML defines a common Extensible Markup Language (XML) framework for exchanging assertions between entities to define, enhance, and maintain a standard XML-based framework for creating and exchanging authentication and authorization information. SAML requires agreements between source and destination sites about information such as Uniform Resource Locators (URLs), source and destination IDs, certification and keys, and other information in the form of metadata. This standard captures the metadata in a standard format as attributes used by SAML entities. The entities define Identity Providers, Service Providers, Attribute Authorities, Attribute Consumers, Authorization Decision Authorities, and Affiliate Members.</p>	<p>SAML Standards</p>
<p>Security and Privacy</p>	<p>Enterprise Privacy Authorization Language (EPAL) – W3C</p>	<p>EPAL goes beyond an application and lays out a standard to protect customers’ and citizens’ private information enterprise wide. Customer and citizen information should be private and secure based on a global enterprise-wide privacy policy. The enterprise privacy policy defines a set of rules where each rule can allow a set of data users to perform an action in a set of actions on a category in a set of categories for any purpose(s).</p>	<p>EPAL W3C</p>
<p>Security and Privacy</p>	<p>WS-Trust Model</p>	<p>This standard takes the Liberty Alliance Trust Guidance reviewed by a broader, more inclusive community. Most concepts are the same as the earlier Liberty Alliance Trust Guidelines.</p>	<p>WS-Trust Model</p>
<p>Security and Privacy</p>	<p>eAuthentication and use of services Object Management Group (OMG) initiative</p>	<p>The OMG initiative is an additional security team with FEA SPP. This team is considering extending and adding additional security and privacy services. The United States Department of Agriculture (USDA)</p>	<p>The OMG Initiative</p>

		has established an eAuthentication setup. Organization for the Advancement of Structured Information Standards (OASIS) tested and proved the E-Gov eAuthentication initiative using WS-* standards.	
Security and Privacy	Public Key Infrastructure (PKI)	This standard describes how communities share policies and authorization schemes based on sharing attributes known as proxy credentials. It enables entity A to grant entity B the authorization right with others as if it were A. This profile allows limited proxy by providing a framework for carrying policies in Proxy Certificates. X.509 Public Key Infrastructure (X.509) started in 1988. Since that time, several Requests for Comments (RFC) exist for the X.509 standard specifying formats for public key certificates, certificate revocation lists, attribute certificates, and certification path validation algorithm. RFC 3820 is the most popular.	Public Key Infrastructure
Security and Privacy	Health Security	ISO/International Electrotechnical Commission (IEC) 27002:2013 <i>Code of practice for information security controls</i> . Standards and Certification Criteria for Electronic Health Records (EHR). Metadata Standards to Support Nationwide Electronic Health Information Exchange.	ISO Health Security Standards
Security and Privacy	Unified Modeling Language (UMLsec) and Security Engineering Profiles	UMLsec is an extension to the Unified Modelling Language for integrating security related information in UML specifications. This information can be used for model-based security engineering. Efforts to create new security stereotypes to integrate them with the UML 2.0 activity diagrams along with other formal Message Sequence Chart extensions.	Presenting the Profile to the Object Modeling Group

Security and Privacy	Security and Privacy Data Content Labeling and XML Access Authorization	Oracle Labeling Security has strong appeal, and there is extensive background information on distributed labeling (e.g., the work at Cornell by Andrew Meyers, et al). This is necessary for crossline of business security and privacy control.	Security and Privacy Data Content Labeling
Security and Privacy	Consumer Health Informatics (CHI) Initiatives	CHI is a Kaiser Foundation Model that assists in minimizing the gap between patients and health resources. HITECH and other initiatives have grown from this model. There are a variety of sources for standards: <ul style="list-style-type: none"> · Electronic Health Records Systems (EHR-S) · NwHIN 	CHI Initiatives
Security and Privacy	Identity Management	The purpose of the Identity Management rule is to ensure that Identity Management Services provide secure, reliable and interoperable mechanisms for authenticating the identity of devices, application services, and Users that consume state information and application resources. This rule is modeled after the Identity Ecosystem Framework Baseline Functional Requirements v1.0, October 15, 2015.	Florida Security Rules
Security and Privacy	Federal Information Processing Standards (FIPS) 140-2	U.S. Government standard to approve cryptographic modules, functions, and algorithms that defines four levels of security: Level 1 - Basic security with one approved algorithm or function and no physical security mechanism Level 2 - Enhanced physical and tamper detection requirements Level 3 - Tamper resistant and mitigation requirements for Critical Security Parameters (CSP) to detect and respond to attempted access or modification of cryptographic modules Level 4 - Provides complete tamper and physical protection. Intended for cryptographic operation in open or uncontrolled environments with	FIPS 140-2

		protection features for environmental and operational fluctuations	
Security and Privacy	Physical Access and Security	The purpose of this rule development is to provide operational management and oversight regarding the state data center.	Florida Rules on Physical Security
Security and Privacy	Web Security Best Practices	The purpose of this document is to ensure that the applications developed in-house or bought off-the-shelf adhere to and enforce the security requirements needed to make the application function in a secure manner and free from flaws that could be exploited.	Web Security
Security and Privacy	SSO Access Controls Standards and Procedures	The purpose of this document is to ensure adherence to CJIS Security Policy and regulate user access to data and the extent of each user's access.	SSO Access Control Standards
Security and Privacy	NIST Framework to HIPAA Security	This crosswalk document identifies <i>mappings</i> between NIST's Framework for Improving Critical Infrastructure Cybersecurity and the HIPAA Security Rule.	NIST Framework for HIPAA
Security and Privacy	Public Key Infrastructure (PKI)	x.509 Certification Standard	PKI x.509 Certification Standards
Security and Privacy	Universal 2nd Factor (U2F)	The FIDO U2F protocol enables relying parties to offer a strong cryptographic 2nd factor option for end user security. The relying party's dependence on passwords is reduced. The password can even be simplified to a 4-digit PIN.	FIDO U2F
Security and Privacy	Security Assertion Markup Language 4 (SAML)	This specification defines the syntax and semantics for XML-encoded assertions about authentication, attributes, and authorization, and for the protocols that convey this information.	SAML 4
Service Interoperability	Kerberos Network Authentication Service	This document describes the concepts and model upon which the Kerberos network authentication system is based. It also specifies Version 5 of the Kerberos protocol.	Kerberos Network Authentication Service

Service Interoperability	OAuth 2.0 authorization framework	The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.	OAuth 2.0 Framework
Service Interoperability	UAF	The FIDO UAF strong authentication framework enables online services and websites, whether on the open Internet or within enterprises, to transparently leverage native security features of end-user computing devices for strong user authentication and to reduce the problems associated with creating and remembering many online credentials. The FIDO UAF Reference Architecture describes the components, protocols, and interfaces that make up the FIDO UAF strong authentication ecosystem.	FIDO UAF
Security and Privacy	WS-Security Rights Expression Language (REL) Token Profile	This document describes how to use ISO/IEC 21000-5 Rights Expressions with the Web Services Security (WSS) specification. This document integrates specific error corrections or editorial changes to the preceding specification, within the scope of the Web Services Security and this TC. This document introduces a third digit in the numbering convention where the third digit represents a consolidation of error corrections, bug fixes, or editorial formatting changes (e.g., 1.1.1); it does not add any new features beyond those of the base specifications (e.g., 1.1).	WS-Security REL Token Profile
Security and Privacy	WS-Security Policy	This document indicates the policy assertions for use with [WS-Policy] which apply to WSS: SOAP Message Security [WSS10, WSS11], [WS-Trust] and [WS-Secure Conversation]. This document incorporates Approved Errata	WS-Security Policy

		approved by the Technical Committee on April 25, 2012.	
Security and Privacy	WS-Trust	WS-Trust 1.4 defines extensions that build on [WS-Security] to provide a framework for requesting and issuing security tokens, and to broker trust relationships. This document incorporates errata approved by the Technical Committee on April 25, 2012.	WS-Trust
Security and Privacy	Secure Sockets Layer (SSL) Protocol	This document specifies version 3.0 of the Secure Sockets Layer (SSL 3.0) protocol, a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.	SSL Protocol
Security and Privacy	Transport Layer Security (TLS)	This memo describes how to use TLS to secure HTTP connections over the Internet. Current practice is to layer HTTP over SSL (the predecessor to TLS), distinguishing secured traffic from insecure traffic by the use of a different server port. This document documents that practice using TLS. A companion document describes a method for using HTTP/TLS over the same port as normal HTTP.	Transport Layer Security
Security and Privacy	Florida Cybersecurity Standards (FCS).	This rule establishes cybersecurity standards for information technology (IT) resources. These standards are documented in Rules 60GG-2. State Agencies must comply with these standards in the management and operation of state IT resources. This rule is modeled after the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.	Florida Cybersecurity Standards
Security and Privacy	Health Information Portability and Accountability Act (HIPAA) Security Rule	Regulation developed by the U.S. Health and Human Services to protect the privacy and security of personal health information (PHI). (45 C.F.R. Subpart C, Part 164)	HIPAA Security Rule on Government Publishing Office

Security and Privacy	Federal Information Security Modernization Act (FISMA) of 2014	Establishes Secretary of Homeland Security as the responsible party to implement policies and practices to secure Federal Information Systems. (44 U.S.C. §2521)	FISMA 2014 on Government Publishing Office
Architecture, Analysis and Design Standards	National Institute of Standards and Technology Cybersecurity Framework for Critical Infrastructure	Voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risk. Developed in accordance with Executive Order 13636 <i>Improving Critical Infrastructure Cybersecurity</i> and the Cybersecurity Enhancement Act of 2014 (15 U.S.C. §7421) to maintain efficient, innovative secure, and resilient Federal Information Systems.	NIST Cybersecurity Framework (CSF)
Security and Privacy	Florida Information Protection Act of 2014	A security law that requires covered entities to notify and disclose information breaches to Personally Identifiable Information (PII) of Florida Residents. (F.S. §501.171)	Florida Information Protection Act of 2014
Architecture, Analysis and Design Standards	Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS)	An open source standard that defines classification tiers, based on the communications and information patterns of the application, and provides lists of application security configurations and tests available to architects, designers, testers, and analysts. The controls defined within the framework enable a standardized evaluation of module application security and risk management related to application vulnerabilities.	OWASP 3.0 ASVS Landing Page
Data Standards	Data Encryption	Standards for the encryption and protection of information.	
Security and Privacy	Business Associate Agreement	Provisions constitute a business associate agreement for purposes of complying with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Is applicable if the Vendor is a business associate within the meaning of the Privacy and Security Regulations, 45 C.F.R. 160 and 164.	Business Associate Agreement

Security and Privacy	Sharing of PHI & PII	Any confidential personal identity information (PII) and individually identifiable health information (PHI) is not transported outside the United States in all vendor or their subcontractors' related business processes.	
Architecture, Analysis and Design Standards	SAMM (Software Assurance Maturity Model)	The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.	OWASP SAMM
Development	CWE (Common Weakness Enumeration)	CWE™ is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.	CWE
Security and Privacy	NVD (National Vulnerability Database)	The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.	NVD
Service Interoperability	Security Content Automation Protocol (SCAP)	The Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans. This publication, along with its annex (NIST Special Publication 800-126A) and a set of schemas, collectively define the technical composition of SCAP version 1.3 in terms of its component specifications, their interrelationships and interoperation,	SCAP

		and the requirements for SCAP content.	
Testing	OWASP Testing Guide	This project's goal is to create a <i>best practices</i> web application penetration testing framework which users can implement in their own organizations and a <i>low level</i> web application penetration testing guide that describes how to find certain issues.	OWASP Testing Guide
Security and Privacy	National Institute of Standards and Technology (NIST) Initiatives	NIST has a variety of initiatives to address IT standards. Some of these initiatives include: <ul style="list-style-type: none"> · Computer Security · Cloud Computing · Biometrics · Data and Informatics · Health IT · Information Delivery 	NIST Initiatives
Service Interoperability	Accredited Standards Committee X12 (ASC X12)	ASC X12, chartered by the American National Standards Institute, develops and maintains Electronic Data Interchange (EDI) and Context Inspired Component Architecture (CICA) standards along with Extensible Markup Language (XML) schemas that drive business processes globally.	ASC X12
Architecture, Analysis and Design Standards	Health Level 7 (HL7)	HL7 is the global authority on standards for interoperability of health information technology with members in over 55 countries.	HL& Standards
Service Interoperability	National Council for Prescription Drug Programs (NCPDP)	NCPDP standards apply to ordering drugs from retail pharmacies. They standardize information between healthcare providers and pharmacies.	NCPDP Standards
Service Interoperability	National Information Exchange Model (NIEM)	This is a national program supported by the Federal Government that provides a community of users, tools, common terminology, governance, methodologies, and support that enablers enterprise-wide information exchange.	NIEM Standard
Architecture, Analysis and Design	American Dental Association (ADA)	Works with others to develop and maintain the Code on Dental Procedures and Nomenclature	ADA Nomenclature

Standards		(CDT).	
Data Standards	National Committee on Vital and Health Statistics (NCVHS)	Acts as the public advisory body to Department of Health and Human Services (HHS) for health data and statistics. The NCVHS Standards Subcommittee focuses on healthcare standards.	NCVHS
Data Standards	Workgroup for Electronic Data Interchange (WEDI)	WEDI is the leading authority on the use of Health IT to improve healthcare information exchange to enhance the quality of care, improve efficiency, and to reduce costs of the American healthcare system.	WEDI
Data Standards	Dental Content Committee of the ADA (DeCC)	A committee of the ADA that sets standards for dental claim data content and maintains the Current Dental Terminology (CDT) Codes.	DeCC of the ADA
Data Standards	National Uniform Billing Committee (NUBC)	Formed in 1975 to develop and maintain a single billing form and standard data set to be used nationwide by institutional, private, and public providers and payers for handling healthcare claims.	NUBC
Data Standards	National Uniform Claim Committee (NUCC)	Committee chaired by the American Medical Association (AMA) in partnership with CMS. Membership includes state and national level representatives from Medicaid (including CMS and National Association of Medicaid Directors (NAMDD)) and public health representatives. Maintains the data set for the professional claim.	NUCC
Data Standards	American National Standards Institute (ANSI)	Serves as the U.S. member to the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), coordinating the U.S. position in the development of standards.	ANSI Standards
Data Standards	Organization for the Advancement of Structured Information Standards (OASIS)	Produces worldwide standards for security, Web services, XML conformance, business transactions, electronic publishing, topic maps, and interoperability within and between marketplaces.	OASIS

Data Standards	Office of the National Coordinator for Health Information Technology (ONC)	Federal entity responsible for the nationwide coordination efforts to implement and use state of the art health information technology. Charged with responsibility to coordinate electronic exchange of health information.	ONC
Data Standards	Public Health Data Standards Consortium (PHDSC)	Non-profit membership-based organization of federal, state, and local health agencies; professional associations; academia; public and private sector organizations; international members; and individuals whose goal is to empower the healthcare and public health communities with health information technology standards to improve individual and community health.	PHDSC
Data Standards	Committee E31 on Healthcare Informatics (ASTM 31)	Develops standards related to the architecture, content, storage, security, confidentiality, functionality, and communication of information used within health care.	ASTM 31
Service Interoperability	Object Management Group (OMG)	The OMG is an international, open membership, not-for-profit technology standards consortium, founded in 1989. OMG standards are driven by vendors, end-users, academic institutions, and government agencies. OMG Task Forces develop enterprise integration standards for a wide range of technologies and an even wider range of industries.	OMG Standards
Architecture, Analysis and Design Standards	Unified Modeling Language (UML) Profiles	This standard addresses business specific needs and technologies. The profiles include: Platform Independent Model (PIM), Platform Specific Model (PSM), CORBA Component Model (CCM), Enterprise Application Integration (EAI), Enterprise Distributed Object Computing (EDOC), Modeling Quality of Service (QoS) and Fault Tolerance Characteristics and Mechanisms, Schedule ability, Performance, and Time.	UML Profiles

Architecture, Analysis and Design Standards	Meta-Object Facility (MOF)	This standard provides an environment where models can export from one application, import into another, transport across a network, store in a repository, and then stakeholders can retrieve and render it into different formats.	OMG Meta-Object Facility
Architecture, Analysis and Design Standards	Model Driven Architecture (MDA)	This standard unifies development from a PIM to a PSM. Object Management Group (OMG) MOF-enabled transformations are the basis of this standard.	OMG Model Driven Architecture
Architecture, Analysis and Design Standards	Business Process Definition Metamodel (BPDM)	This standard provides the ability to model business process with standard language and metadata.	OMG Business Process Definition Metamodel
Architecture, Analysis and Design Standards	UML Enterprise Distributed Object Computing (EDOC)	This standard simplifies development of component-based systems using a modeling framework in UML.	OMG EDOC
Architecture, Analysis and Design Standards	Web Ontology Language (OWL-S)	Applications that process content of information rather than presenting information to humans use this standard. It facilitates machine interpretability of web content.	Web Ontology Languages
Architecture, Analysis and Design Standards	Web Service Description Language (WSDL)	WSDL is an Extensible Markup Language (XML) format that describes services as endpoints. It abstractly describes the operations and messages bound by concrete protocols.	WSDL
Architecture, Analysis and Design Standards	Universal Business Language (UBL)	UBL is a normative set of XML schema design rules and naming conventions that coincide with Electronic Business XML (ebXML) Core Components Technical Specifications.	UBL
Architecture, Analysis and Design Standards	WS-Composite Application Models (WS-CAF)	WS-CAF defines a generic and open framework for applications containing multiple services.	OASIS

<p>Architecture, Analysis and Design Standards</p>	<p>Representation State Transfer (REST) Architecture - Web Services</p>	<p>A RESTful web service (also called a RESTful web API) is a simple web service implemented using HTTP and the principles of REST. The REST Web is the subset of the WWW (based on HTTP) in which agents provide uniform interface semantics – essentially create, retrieve, update, and delete – rather than arbitrary or application-specific interfaces, and manipulate resources only by the exchange of representations. Furthermore, the REST interactions are <i>stateless</i> in the sense that the meaning of a message does not depend on the state of the conversation.</p>	<p>REST Web Services</p>
<p>Architecture, Analysis and Design Standards</p>	<p>Web Services Modeling Ontology (WSMO)</p>	<p>WSMO describes aspects of a Semantic Web with four main elements:</p> <ul style="list-style-type: none"> · Ontology’s for terminology · Intention goals · Web service descriptions · Mediators 	<p>WSMO</p>
<p>Architecture, Analysis and Design Standards</p>	<p>National Human Service Interoperability Architecture (NHSIA)</p>	<p>NHSIA proposes a framework to facilitate information sharing, improve service delivery, prevent fraud, and provide better outcomes for children and families.</p>	<p>NHSIA</p>
<p>Service Interoperability</p>	<p>Extensible Markup Language (XML)</p>	<p>XML is a simple, flexible text format derived from Standard Generalized Markup Language (SGML). This standard provides a variety of associated standards, such as:</p> <ul style="list-style-type: none"> · Associating Schemas · XQuery · Efficient XML Interchange · Extensible Stylesheet Language (XSL) Transformations (XSLT) – document transformation and presentation, XSL Formatting Objects (XSL-FO), and eXtended Memory Specification (XMS) Path Language 	<p>XML</p>
<p>Service Interoperability</p>	<p>Simple Object Access Protocol (SOAP)</p>	<p>This is a protocol for the exchange of information. It does not define application semantics, but a simple mechanism for expressing application semantics.</p>	<p>W3C</p>

Service Interoperability	SOAP with attachments-Message Transmission Optimization Mechanism (MTOM)	SOAP with attachments allows a message to contain attachments and provides rules for Uniform Resource Identifier (URI) references.	SOAP
Service Interoperability	Universal Description, Discovery, and Integration (UDDI)	UDDI is a platform independent extensible markup language registry. Originally, proposed as a core web service standard, it interrogates SOAP messages to provide WSDL protocol bindings and message formats.	UDDI
Service Interoperability	Hypertext Transfer Protocol (HTTP)	Networking protocol for distributed, information systems. The Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) develop these standards. HTTP is a request-response protocol for client-server models.	HTTP
Service Interoperability	Hypertext Transfer Protocol – Secure (HTTPS)	HTTPS combines HTTP with Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol to provide encrypted communications and secure identification.	HTTPS
Service Interoperability	Web Services Description Language (WSDL)	This is a messaging standard in XML format for describing network services as endpoints. The messages are either document-oriented or procedure-oriented information. The messages bind to the concrete network protocol.	WSDL
Security and Privacy	Electronic Business XML (ebXML) Registry	This standard provides interoperable registries and repositories with an interface that enables submission, query, and retrieval.	ebXML
Service Interoperability	WS-Policy	The WS-Policy provides a general-purpose model and corresponding syntax to describe and communicate the policies of a web service. WS-Policy defines a base set of constructs used and extended by other web services specifications to describe a broad range of service requirements, preferences, and capabilities.	WS-Policy

Service Interoperability	WS-Agreement	Standards are at varying levels of maturity. Some standards are ready for use today, some are emerging, and others are in a stage referred to as <i>incubating</i> . The term incubating describes a standard that is developing convergence and may require 3 to 5 years before finalization and adoption.	WS-Agreement
Service Interoperability	WS-Addressing	This is a key element in the definition of a complete process flow. Middleware and service-delivery companies have an interest in this standard because it is one of the key elements for adding more resource definition information to the URI points. It currently consists of three major pieces: · Core · SOAP binding · WSDL binding with WSDL 2.0	WS-Addressing
Service Interoperability	WS-Reliability	WS-Reliability is a SOAP-based protocol for exchanging SOAP messages with guaranteed delivery, no duplicates, and guaranteed message ordering. WS-Reliability is SOAP message header extensions and is independent of the underlying protocol. It includes a binding to HTTP. The focus is on Business-to-Business (B2B) reliable message delivery. The specification borrows from previous work in messaging (e.g., ebXML) and transports and applies to WS services.	WS-Reliability
Service Interoperability	Structured Query Language (SQL)	A database computer declarative language designed for managing data in relational database management systems.	ANSI SQL
Service Interoperability	XML Schema	Other developers who are building their own special-purpose application use these sets of standard application elements.	W3C XML Schema

Service Interoperability	Service Level Agreement Language (SLAng)	SLAng records a common understanding about services, priorities, responsibilities, and other contractual items. The SLAng contains segments for address, service definitions, performance, problem management, customer duties, warranties, disaster recovery, and agreement termination. Specific examples include Web Service Level Agreement Language for Collaborations (WSLA+), Cloud Computing, and Backbone Internet providers.	SLAng
Service Interoperability	Web Service Distribution Management (WSDM)	WSDM is a web service standard for managing and monitoring the status of other services. It contains two specifications: <ul style="list-style-type: none"> · Management Using Web Services (MUWS) defines a basic set of manageability capabilities. · Management of Web Services (MOWS) defines how to manage web services as resources. 	WSDM
Service Interoperability	WS-Reliable Messaging (WSRM)	A protocol that allows reliable delivery of SOAP messages to distributed applications.	WSRM
Service Interoperability	IT Infrastructure Library (ITIL) – IT Service Management Capabilities Level	This is an IT management standardization effort to understand and compare the IT resource utilization and to improve the effectiveness and efficiency of the infrastructure used.	ITIL
Service Interoperability	Distributed Management Task Force (DMTF)	DMTF worked on infrastructure management and has developed a series of standards that are gaining acceptance in the system management industry segment.	DMTF
Service Interoperability	Common Information Model (CIM)	CIM is an object-oriented model that describes the conceptual framework for describing management data. CIM messages are in XML format and over HTTP. CIM messages are well-defined request or response data packets used to exchange information between CIM products.	DMTF CIM

Security and Privacy	Federal Enterprise Architecture Security and Privacy Profile (FEA SPP)	FEA SPP is a scalable and repeatable methodology for addressing information security and privacy from a business-centric perspective. The documentation is at a high level. It does not replace other security and privacy standards but seeks to work across the enterprise.	FEA SPP
Security and Privacy	HIPAA Security and Privacy Rule	The HIPAA Privacy Rule establishes national standards to protect health information. It requires specific safeguards, establishes personal health information, and sets limits and conditions on the disclosure of information.	HIPAA Security and Privacy Rule
Security and Privacy	WS-Security – WS-I Security Profile	The standard enhances the SOAP messaging to provide message integrity and confidentiality. This supports a variety of security models and encryption technologies. It provides a general approach of associating a security token allowing support for multiple token formats. It describes how to encode binary security tokens and describe the tokens associated with a message.	WS-I Security Profile
Business Enabling Technologies	Business Process Model and Notation (BPMN) previously known as Business Process Modeling Notation Business Motivation Model (BMM)	The computer industry consolidated all Business Process Model (BPM) activities under Object Management Group (OMG). The BPMN is a standard for business process modeling that provides a graphical notation for specifying business processes. The BMM specification provides a scheme for developing, communicating, and managing business plans; while BPMN provides a formal mechanism that maps business process to appropriate execution format (BPM).	OMG BPMN and BMM
Business Enabling Technologies	Extensible Markup Language (XML) Forms (XForms)	XForms is an XML application that integrates into other markup languages. XForms gathers and processes XML data using an architecture that separates presentation, purpose, and content. XForms accommodates form component reuse, fosters strong data type validation, eliminates	XML Forms

		unnecessary roundtrips to the server, and offers device independence.	
Business Enabling Technologies	Rule Markup Language (RuleML) Initiative	This is an international non-profit organization covering all aspects of web rules and their interoperation. There are Structure and Technical Groups that focus on RuleML specifications, tools, and application development.	RuleML
Business Enabling Technologies	Workflow Management Coalition (WfMC)	WfMC is a global organization that contributes to process related standards and educates users. Wf-XML and XPDL are leading process definition languages. The coalition also works to provide process simulation and optimization standards.	WfMC
Business Enabling Technologies	Customer Relationship Management (CRM) Extended Relationship Management (xRM)	xRM is the principle and practice of applying CRM and is a standardized interchangeable relationship for services.	
Architecture, Analysis and Design Standards	Technical Document Naming Standards	The Technical Documentation Standards describe the standards that need to be adhered to for documenting Pages, Panels, Reports, etc.	FL MMIS Technical Document Naming Standards
Architecture, Analysis and Design Standards	AUTOSYS Design and Documentation Standards	MMIS Design and Documentation Standards for the AUTOSYS job scheduler.	FL MMIS AUTOSYS Design and Documentation Standards
Architecture, Analysis and Design Standards	Technical Design Documentation	Part of a developer's processes and procedures for MMIS.	FL MMIS Technical Design Documentation
Architecture, Analysis and Design Standards	C Programming Standards	MMIS document setting standards for developers.	FL MMIS C Programming Standards
Architecture, Analysis and Design Standards	C Programming	A general-purpose, imperative computer programming language, supporting structured programming, lexical variable scope and recursion, while a static type system prevents many unintended operations.	C Programming

Architecture, Analysis and Design Standards	.NET Programming Standards	MMIS .Net Programming Standards.	FL MMIS .Net Programming Standards
Architecture, Analysis and Design Standards	.NET Programming Standards	This is the .NET Programming Standards and guidelines.	.NET Programming Standards
Project Documentation	Defect Documentation Standards	Standards for documenting defects.	FL MMIS Defect Tracking Standards
Service Interoperability	Integration Standards	Proposed integration standards being developed by DMS will modify Rule 60GG-5.	
Architecture, Analysis and Design Standards	. Net Framework Coding Standards	The purpose of this document is to identify net framework coding standards that should be followed for all .net applications that are developed by (IT) staff and augmented staff.	AHCA .NET Programming Standards
Architecture, Analysis and Design Standards	C# programming Standards	The purpose of this document is to provide coding style standards for the development of source code written in C sharp. Adhering to a coding style standard is an industry proven best practice for making team development more efficient and application maintenance more cost effective. These guidelines represent the minimum level of standardization expected in the source code of all projects written in C sharp.	C# Programming Standards
Architecture, Analysis and Design Standards	Application Patches Testing Standards	The purpose of this document is to provide a core set of standards and principles that can be used to maintain an effective patch/update test management program in a systematic way.	AHCA Application Testing Standards
Architecture, Analysis and Design Standards	Application Code Review and Promotion Procedures	The purpose of this document is to document the code review process for any application/reports/web service developed or maintained within AHCA. A code review consists of a review of an application's design, functionality, connections, and code.	AHCA Code Review and Promotion Procedures

Architecture, Analysis and Design Standards	Web Forms Standards	The purpose of this document is to provide a guide that illustrates step by step instructions to create web forms.	Web Forms Standards
Architecture, Analysis and Design Standards	SQL Server Standards	The purpose of this document is to identify SQL coding standards that should be followed for all SQL applications that are developed by (IT) staff and augmented staff. Source code location and version information must be documented and maintained in Visual Studios T.F.S.	AHCA SQL Server Standards
Architecture, Analysis and Design Standards	SharePoint Standards and Procedures	The purpose of this document is to ensure that the system is managed and used in accordance with the design and intent to avoid creating an unusable and unmanaged system.	AHCA SharePoint Standards
Architecture, Analysis and Design Standards	.Net Development Servers	The purpose of this document is to ensure all developers are aware that the old servers are now obsolete. All .net development servers have been migrated to the cloud.	.NET Development Servers
Architecture, Analysis and Design Standards	CRM Standards and Procedures	The purpose of this document is to ensure that the system is managed and used in accordance with the design and intent to avoid creating an unusable and unmanageable system. This document should be read by all people that use, support, and enforce the system.	CRM Standards and Procedures
Architecture, Analysis and Design Standards	AHCA SSRS Report Writing Standards and Procedures	The purpose of this document is to ensure that the SSRS report writing process is managed in accordance with the vision's intent to avoid creating an unusable and manageable process while following Agency policy and development best practices.	AHCA SSRS Report Writing Standards
Architecture, Analysis and Design Standards	Name Checker	The Name Checker Utility is a tool which performs data name translation and data name compliance analysis. These two functions implement the CMS Data Administration Standards, Guidelines, and Operating Procedures as they apply to forming valid names of data entities, data attributes, database tables, and	CMS Name Checker Utility

		database columns. The tool employs the CMS Data Administration Glossary of Standard Terms and Abbreviations.	
Service Interoperability	Simple Object Access Protocol (SOAP)	Soap Version 1.2 Framework	FL Rules SOAP
Service Interoperability	WS-Policy	The Web service specifications (WS*) are designed to be composed with each other to provide a rich set of tools for secure, reliable, and/or transacted Web services. WS-Policy by itself does not provide a negotiation solution for Web services. WS-Policy is a building block that is used in conjunction with other Web service and application-specific protocols to accommodate a wide variety of policy exchange models.	WS-Policy
Service Interoperability	WS-SecureConversation	This specification defines extensions to allow security context establishment and sharing, and session key derivation. This allows contexts to be established and potentially more efficient keys or new key material to be exchanged, thereby increasing the overall performance and security of the subsequent exchanges.	WS-SecureConversation
Service Interoperability	JavaScript Object Notation (JSON)	JSON (JavaScript Object Notation) is a lightweight data-interchange format. It is easy for humans to read and write. It is easy for machines to parse and generate. It is based on a subset of the JavaScript Programming Language.	JSON
Service Interoperability	Hypertext Transfer Protocol (HTTP)	The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, and hypertext information systems.	HTTP

<p>Service Interoperability</p>	<p>Secure Shell (SSH) Transport Layer Protocol</p>	<p>SSH is a protocol for secure remote login and other secure network services over an insecure network. This document describes the SSH transport layer protocol, which typically runs on top of TCP/IP. The protocol can be used as a basis for secure network services. It provides strong encryption, server authentication, and integrity protection. It may also provide compression.</p>	<p>SSH Transport Layer Protocol</p>
<p>Service Interoperability</p>	<p>Domain Name System (DNS) Protocol</p>	<p>The goal of domain names is to provide a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internets, and administrative organizations.</p>	<p>DNS Protocol</p>
<p>Service Interoperability</p>	<p>XML Configuration Access Protocol (XCAP)</p>	<p>This specification defines the Extensible Markup Language (XML) Configuration Access Protocol (XCAP). XCAP allows a client to read, write, and modify application configuration data stored in XML format on a server. XCAP maps XML document sub-trees and element attributes to HTTP URIs, so that these components can be directly accessed by HTTP.</p>	<p>XCAP</p>
<p>Architecture, Analysis and Design Standards</p>	<p>Uniform Resource Identifier (URI)</p>	<p>A URI is a compact sequence of characters that identifies an abstract or physical resource. This specification defines the generic URI syntax and a process for resolving URI references that might be in relative form, along with guidelines and security considerations for the use of URIs on the Internet. The URI syntax defines a grammar that is a superset of all valid URIs, allowing an implementation to parse the common components of a URI reference without knowing the scheme-specific requirements of every possible identifier. This specification does not define a generative grammar for URIs; that task is performed by the individual specifications of each URI</p>	<p>URI Standard</p>

		scheme.	
Service Interoperability	Resource Description Format (RDF)	The RDF is a framework for representing information in the Web. RDF Concepts and Abstract Syntax defines an abstract syntax on which RDF is based, and which serves to link its concrete syntax to its formal semantics. It also includes discussion of design goals, key concepts, data typing, character normalization, and handling of URI references.	Resource Description Framework
Service Interoperability	Web Application Description Language (WADL)	This specification describes the Web Application Description Language (WADL). An increasing number of Web-based enterprises (Google, Yahoo, Amazon, Flickr to name but a few) are developing HTTP-based applications that provide programmatic access to their internal data. Typically, these applications are described using textual documentation that is sometimes supplemented with more formal specifications such as XML schema for XML-based data formats. WADL is designed to provide a machine process-able description of such HTTP-based Web applications.	WADL
Architecture, Analysis and Design Standards	Data Center Usage Agency Limitations	(5) AGENCY LIMITATIONS.— (a) Unless exempt from data center consolidation pursuant to this section or authorized by the Legislature or as provided in paragraph (b), a state agency may not: 1. Create a new agency computing facility or data center, or expand the capability to support additional computer equipment in an existing agency computing facility or data center; 2. Spend funds before the state agency's scheduled consolidation into the state data center to purchase or modify hardware or operations software that does not comply with standards established by the Agency for State Technology pursuant to s. 282.0051; 3. Transfer existing computer services to any data center other than the state data center;	Florida Statue 282.201

		<p>4. Terminate services with the state data center without giving written notice of intent to terminate services 180 days before such termination; or</p> <p>5. Initiate a new computer service except with the state data center.</p>	
--	--	---	--

APPENDIX D: INBOUND AND OUTBOUND INTERFACES

INBOUND INTERFACES FMMIS/DSS

<p>Agency for Health Care Administration</p> <p>Provider Rate file, Mandatory Assignment and enrollment data from AHS, Recipient HIV AIDS data, Recipient SMI data, Disease Management Recipient File, Updated capitation rates, Nursing Home rate file, Intermediate Care Facility rate file, Hospice rate file, Provider rate file, Provider DRG rate file, ASC rate file, KICK rate file, LEIE Monthly Updates</p>	<p>Electronic Data Interchange</p> <p>FHK 270/271 Match files with Reports, X12 837 5010 Claims institutional encounters, X12 837 5010 Claims dental encounters, X12 837 5010 Claims professional encounters, X12 837 5010 Claims institutional, X12 270 5010 Health Care Eligibility request, X12 276 5010 Claim Status request, X12 837 5010 Claims dental, X12 837 5010 Claims professional</p>	<p>Health Quality Assurance</p> <p>HQA License file update the Facility provider license information, HQA Modifier file match providers to valid license numbers, HQA Status Code file, HQA Address Type Codes, HQA Client Codes, HQA Ownership Codes, HQA modifier Codes</p>	<p>Centers for Medicare & Medicaid Services</p> <p>COBA response files from CMS, Medicare Part D data, EDB database of CMS-oriented recipients (Medicare A/B/D and Medicare Buy-In), Medicare Part A billing information, Medicare Part B billing information, Medicare Part D enrollment information, CMS (HCFA) file used to update CLIA table record types 1, 3 and 5, NCCI Interface Professional NCCI edits, NCCI Interface Hospital NCCI edits, MUE Interface Professional MUE edits, MUE Interface DME MUE edits, HCPCS Interface HCPCS procedure codes, ICD10 interface add/update ICD10 Diagnosis and Procedure codes</p>
<p>Automated Health Systems Provider Plan Network File</p>	<p>EQ Health</p> <p>Home Health Prior Authorization, Inpatient Prior Authorization, PPEC Prior Authorization, Professional Therapy Prior Authorization, Outpatient Therapy Prior Authorization, DME Prior Authorization, Dental Prior Authorization, Vision Prior Authorization, Hearing Prior Authorization, Physician Prior Authorization, Inpatient Psychiatric Prior Authorization, SIPP Inpatient Psychiatric Prior Authorization, Outpatient Prior Authorization</p>	<p>Magellan</p> <p>Prior authorization data for drug claims, Magellan sends contact information, Magellan sends adjudicated claims, Magellan Formulary coverage for drugs, Magellan State determined Maximum Allowable Cost (SMAC) drugs, Magellan Formulary Extract for Drug Rebate, Magellan SMAC Interface, Magellan Formulary drug termination date, UPC Interface used to add/update UPC codes</p>	<p>Department of Juvenile Justice – DJJ incarceration information</p>
<p>Agency for Persons with Disabilities APD Gatekeeper Prior Authorization</p>	<p>NPPES Monthly Master file, NPPES Monthly Deactivation file, NPPES Weekly Updates</p>	<p>Other Inbound Interfaces</p> <p>IRS CP2100 tape Provider B notice created Maximus data from Florida Healthy Kids Maximus Monthly MEC 834 Eligibility file FHK MEUPS PIN Letter file MFAO Physician Fee Schedule rate update MFAO DRG rate update SDX Resource file SSA data file System for Award Management Daily Updates Link Provider add members to Provider Group Wells Fargo Cleared Checks (interChange)</p>	<p>Department of Health</p> <p>DOH License File, Claims using external interface file from Healthy Start, Data files from Florida Bureau of Vital Statistics, DOH Immunization Registry</p>
<p>First Data Bank Update reference configuration data</p>	<p>TPL Vendor Resource file, TPL Vendor Manage adjustments, TPL Vendor Voided claims</p>		<p>Florida Department of Law Enforcement FDLE incarceration information, LiveScan input file</p>

OUTBOUND INTERFACES FMMIS/DSS

<p>Agency for Health Care Administration</p> <p>Drug claims paid for Prepaid Mental Health Plan recipients, Appropriations report generated out of the weekly financial cycle.</p>	<p>Centers for Medicare & Medicaid Services</p> <p>EDB Finder File listing of recipients, Medicare Part A accretions, deletions and demographic changes, Medicare Part B accretions, deletions and demographic changes, COBA monthly extract, Pharmacy Claims file for CMS MMA Plans</p>	<p>EQ Health</p> <p>Extract of professional claims, Extract of UB92 claims, Extract of dental claims, Extract of pharmacy claims, Extract of professional encounter claims, Extract of UB92 encounter claims, Extract of dental encounter claims, Extract of pharmacy encounter claims, Extract of recipient data, Home Health Prior Authorization, Inpatient Prior Authorization, PPEC Prior Authorization, Professional Therapy Prior Authorization, Outpatient Therapy Prior Authorization, DME Prior Authorization, Dental Prior Authorization, Vision Prior Authorization, Hearing Prior Authorization, Physician Prior Authorization, Inpatient Psychiatric Prior Authorization, SIPP Inpatient Psychiatric Prior Authorization, Outpatient Prior Authorization, Provider extract new providers/updates</p>	<p>HMS (TPL Vendor)</p> <p>Resource file from FMMIS/DSS, Carrier file from FMMIS/DSS, Recipient eligibility file from FMMIS/DSS, Lead letter data file from FMMIS/DSS, Pharmacy claims file from FMMIS/DSS, Provider Medicare to Medicaid cross-reference file, Provider file from FMMIS/DSS, Paid dental claims file from FMMIS/DSS, Drug code file from FMMIS/DSS, Procedure code file from FMMIS/DSS, Diagnosis code file, Institutional claim file, Physician claims file from FMMIS/DSS</p>	<p>SAS Extract of recipient data to SAS, Extract new providers or updates, Provider Owner SAS extract file</p> <p>Web Portal Provider Master Listing Extract, Pending Provider Listing Extract e</p>
<p>Automated Health Systems</p> <p>File for determining eligible recipients in reform counties, Recipient data to AHS Choice Counseling, Managed Care data to Enrollment Broker</p>	<p>Department of Children and Families</p> <p>Terminated SDX recipients extract, Recipient FLORIDA Update Error Report & FLORIDA Match Error Report, Carrier data for FLORIDA eligibility, Home Safe Net recipients</p>	<p>Providers/Managed Care Organizations</p> <p>X12 271 5010 Health Care Eligibility, Unsolicited X12 271 5010 HC Eligibility, X12 277 5010 Claim Status response, X12 277U 5010 response from Financial or Claims when information is missing, X12 835 5010 HC Claim Payment Advice, MCO capitations paid enrolled recipients, X12 999 5010 report errors or acknowledge error-free transaction set, X12 997 5010 report errors or acknowledge error-free transaction set</p>	<p>Magellan</p> <p>Recipient data for MMA/TPL information, Pharmacy Claim voids, Claim RetroDUR processing, HPE to Unisys Drug Claims Drug Rebate, HPE to Unisys Drug Extract Drug Rebate, HPE to Unisys Physician UB Claims Drug Rebate, Pharmacy Provider extract First Health 4 files - Address, Panel, On Review, NPI, Header and Trailer records to extract file FLM_PanelData.dat, Header and Trailer records to extract file FLM_PorData_Update.dat, License base and alias files, License address file, License specialty file, Provider License alias file updates</p>	<p>Other Outbound Interfaces</p> <p>MFAO - Provider Type '35' and Specialty '71', '72', '73', '74', '88' Conduent - Receive file from CMS (monthly) and send to TPL vendor CPS - ID Card extract DOH - Extract of HIV recipients DOT - Extract of recipient data First Health - Resource file Healthy Start MomCare Network - HS enrollment data of newly eligible Healthy Start recipients HPE Banking Dept. - Checks issued weekly financial cycle HPE LG Team - Recipient info used for 1095-B forms MCO's - Rosters to MCOs Maximus - Error response file Molina - Monthly Pharmacy Encounter Claim extract Tirion - Providers terminated lock access to web portal or providers need a pin letter or pin reset Unity One - Extract recipient data USF - Delta file SMMC MMA Managed Care recipients and SMMC plans all active MMA enrolled recipients</p>
<p>Agency for Person with Disabilities</p> <p>Extract for new providers or updates, DS Waiver Paid Claims for recipients care plans within APD Gatekeeper Matrix, DS Waiver Denied claims for recipients care plans within APD Gatekeeper Matrix, Weekly claim extract for all paid claims with S9122 TJ procedure code billed, Weekly claim extract for all voided claims with S9122 TJ procedure code billed, Gatekeeper Prior Authorization Interface, Gatekeeper Prior Authorization Summary Report, Gatekeeper Prior Authorization Transaction Listing Report, Interface for EQ Health PA with Procedure code S9122TJ</p>	<p>Department of Elder Affairs</p> <p>All DOEA recipients delimited data file, Monthly Capitation extract, Monthly MP enrollments active as of first of the next month</p>			
<p>Beacon Health</p> <p>Provider Extract for Beacon Extract of recipient data</p>	<p>Medtel</p> <p>Extract of recipient data to MEDTEL, Provider extract for Med_Tel Call Center, Active Providers for Med_Tel</p>			